EXHIBIT C

United States Government Accountability Office

Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

May 2014

VIRTUAL CURRENCIES

Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges

GAO-14-496

GAO Highlights

Highlights of GAO-14-496, a report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

May 2014

VIRTUAL CURRENCIES

Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges

Why GAO Did This Study

Virtual currencies—digital representations of value that are not government-issued—have grown in popularity in recent years. Some virtual currencies can be used to buy real goods and services and exchanged for dollars or other currencies. One example of these is bitcoin, which was developed in 2009. Bitcoin and similar virtual currency systems operate over the Internet and use computer protocols and encryption to conduct and verify transactions. While these virtual currency systems offer some benefits, they also pose risks. For example, they have been associated with illicit activity and security breaches, raising possible regulatory, law enforcement, and consumer protection issues. GAO was asked to examine federal policy and interagency collaboration issues concerning virtual currencies.

This report discusses (1) federal financial regulatory and law enforcement agency responsibilities related to the use of virtual currencies and associated challenges and (2) actions and collaborative efforts the agencies have undertaken regarding virtual currencies. To address these objectives, GAO reviewed federal laws and regulations, academic and industry research, and agency documents; and interviewed federal agency officials, researchers, and industry groups.

What GAO Recommends

GAO recommends that CFPB take steps to identify and participate in pertinent interagency working groups addressing virtual currencies, in coordination with other participating agencies. CFPB concurred with this recommendation.

View GAO-14-496. For more information, contact Lawrance L. Evans, Jr. at (202) 512-8678 or evansl@gao.gov.

What GAO Found

Virtual currencies are financial innovations that pose emerging challenges to federal financial regulatory and law enforcement agencies in carrying out their responsibilities, as the following examples illustrate:

- Virtual currency systems may provide greater anonymity than traditional payment systems and sometimes lack a central intermediary to maintain transaction information. As a result, financial regulators and law enforcement agencies may find it difficult to detect money laundering and other crimes involving virtual currencies.
- Many virtual currency systems can be accessed globally to make payments and transfer funds across borders. Consequently, law enforcement agencies investigating and prosecuting crimes that involve virtual currencies may have to rely upon cooperation from international partners who may operate under different regulatory and legal regimes.
- The emergence of virtual currencies has raised a number of consumer and investor protection issues. These include the reported loss of consumer funds maintained by bitcoin exchanges, volatility in bitcoin prices, and the development of virtual-currency-based investment products. For example, in February 2014, a Tokyo-based bitcoin exchange called Mt. Gox filed for bankruptcy after reporting that it had lost more than $460 million.

Federal financial regulatory and law enforcement agencies have taken a number of actions regarding virtual currencies. In March 2013, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued guidance that clarified which participants in virtual currency systems are subject to anti-money-laundering requirements and required virtual currency exchanges to register with FinCEN. Additionally, financial regulators have taken some actions regarding anti-money-laundering compliance and investor protection. For example, in July 2013, the Securities and Exchange Commission (SEC) charged an individual and his company with defrauding investors through a bitcoin-based investment scheme. Further, law enforcement agencies have taken actions against parties alleged to have used virtual currencies to facilitate money laundering or other crimes. For example, in October 2013, multiple agencies worked together to shut down Silk Road, an online marketplace where users paid for illegal goods and services with bitcoins.

Federal agencies also have begun to collaborate on virtual currency issues through informal discussions and interagency working groups primarily concerned with money laundering and other law enforcement matters. However, these working groups have not focused on emerging consumer protection issues, and the Consumer Financial Protection Bureau (CFPB)—whose responsibilities include providing consumers with information to make responsible decisions about financial transactions—has generally not participated in these groups. Therefore, interagency efforts related to virtual currencies may not be consistent with key practices that can benefit interagency collaboration, such as including all relevant participants to ensure they contribute to the outcomes of the effort. As a result, future interagency efforts may not be in a position to address consumer risks associated with virtual currencies in the most timely and effective manner.

Contents

Abbreviations

BSA	Bank Secrecy Act
BSAAG	Bank Secrecy Act Advisory Group
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
DATA	Digital Asset Transfer Authority
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
ECTF	Electronic Crimes Task Forces
EFTA	Electronic Fund Transfer Act
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
IOC-2	International Organized Crime Intelligence and Operations Center
IRS	Internal Revenue Service
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
SEC	Securities and Exchange Commission
TOR	The Onion Router
USAID	United States Agency for International Development
VCET	Virtual Currency Emerging Threats Working Group

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 29, 2014

The Honorable Thomas R. Carper
Chairman

The Honorable Tom A. Coburn
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

While not widely used or accepted, virtual currencies, such as bitcoin, have grown in popularity in recent years and have emerged for some as potential alternatives to traditional currencies issued by governments. Virtual currencies operate over the Internet and, in some cases, may be used to buy real goods and services and exchanged for traditional currencies. They offer potential benefits over traditional currencies, including lower transaction costs and faster funds transfers. Because some virtual currency transactions provide greater anonymity than transactions using traditional payment systems, law enforcement and financial regulators have raised concerns about the use of virtual currencies for illegal activities. Additionally, recent cases involving the loss of funds from virtual currency exchanges have highlighted potential consumer protection issues.

You asked us to examine potential policy issues related to virtual currencies and the status of federal agency collaboration in this area. This report focuses on the federal financial regulatory agencies and selected federal law enforcement agencies that have a role in protecting the U.S. financial system and investigating financial crimes.[1] Specifically, this report addresses (1) agency responsibilities related to the use of virtual currencies and the emerging challenges these currencies pose to the

[1]Other federal agencies that were outside the scope of this report, such as the Internal Revenue Service (IRS), have responsibilities related to virtual currencies. For example, as we reported in May 2013, IRS is responsible for ensuring taxpayer compliance for all economic areas, including virtual economies and currencies. For more information, see GAO, *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks*, GAO-13-516 (Washington, D.C.: May 15, 2013). In March 2014, IRS determined that virtual currencies will be treated as property for purposes of U.S. federal taxes. Therefore, general tax principles that apply to property transactions apply to transactions using virtual currency. See IRS Notice 2014-21.

agencies; and (2) actions the agencies have taken in response to the emergence of virtual currencies, including interagency collaborative efforts. We selected the law enforcement agencies included in our review based on their involvement in investigating virtual-currency-related crimes and participation in interagency collaborative efforts and congressional hearings on virtual currency issues.

To describe agency responsibilities related to the use of virtual currencies and the emerging challenges these currencies pose, we reviewed the following agency information: testimony and written statements from relevant congressional hearings, written responses to congressional questions, unclassified intelligence assessments, financial reports, training presentations, and descriptions of missions and responsibilities from agencies' websites.[2] We also reviewed prior GAO reports, Congressional Research Service reports, and relevant laws and regulations, including the Bank Secrecy Act (BSA) and related anti-money laundering provisions such as Title III of the USA PATRIOT Act, to gain an understanding of agencies' responsibilities in administering and enforcing anti-money-laundering laws and regulations, as well as in investigating and prosecuting financial and other crimes.[3] In addition, we reviewed academic articles and papers from industry stakeholders. Further, we interviewed officials from the following federal financial regulatory and law enforcement agencies:

- The Board of Governors of the Federal Reserve System (Federal Reserve);
- The Bureau of Consumer Financial Protection (also known as the Consumer Financial Protection Bureau or CFPB);
- The Commodity Futures Trading Commission (CFTC);
- The Department of Homeland Security (DHS), including U.S. Immigration and Customs Enforcement–Homeland Security Investigations (ICE-HSI) and the U.S. Secret Service (Secret Service);

[2]We reviewed testimony and agency statements from two congressional hearings: the November 18, 2013, U.S. Senate Committee on Homeland Security and Governmental Affairs hearing "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies," and the November 19, 2013, U.S. Senate Committee on Banking, Housing, and Urban Affairs hearing, "The Present and Future Impact of Virtual Currency."

[3]Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829(b), 1951-1959; 31 U.S.C. §§ 5311-5330); Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of U.S.C.).

- The Department of Justice (DOJ), including the Criminal Division and two of its components—the Asset Forfeiture and Money Laundering Section and Computer Crime and Intellectual Property Section—and the Federal Bureau of Investigation (FBI);
- The Department of the Treasury (Treasury), including the Financial Crimes Enforcement Network (FinCEN) and the Office of the Comptroller of the Currency (OCC);
- The Federal Deposit Insurance Corporation (FDIC);
- The National Credit Union Administration (NCUA); and
- The Securities and Exchange Commission (SEC).

Additionally, we interviewed an academic whose research focused on virtual currencies and industry stakeholders, including the Bitcoin Foundation, the Digital Asset Transfer Authority (DATA), and the National Money Transmitters Association, which represent the interests of a large number of virtual currency and money transmission businesses.

To examine the actions and collaborative efforts federal agencies have undertaken in response to the emergence of virtual currencies, we reviewed agency information, including FinCEN's regulatory guidance and administrative rulings on the applicability of BSA to virtual currency participants, testimony and written statements from the previously mentioned congressional hearings, written responses to congressional questions, intelligence assessments, a CFPB query of its Consumer Complaint Database, and press releases.[4] We also interviewed officials from the agencies listed previously to obtain further information on the actions they have taken to address the emergence of virtual currencies and their efforts to collaborate with other federal agencies on this issue. Additionally, we interviewed the academic and industry stakeholders noted previously, as well as the Digital Economy Task Force, to determine the extent to which private sector groups were involved in

[4]FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, March 18, 2013; FinCEN, *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001, January 30, 2014; FinCEN, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002, January 30, 2014; and FinCEN, *Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currencies,* FIN-2014-R007, April 29, 2014.

interagency collaborative efforts.[5] We reviewed GAO's key practices on collaboration and assessed whether interagency collaborative efforts related to virtual currencies were consistent with practices concerning the inclusion of relevant participants.[6]

We conducted this performance audit from November 2013 to May 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Virtual currencies are financial innovations that have grown in number and popularity in recent years. While there is no statutory definition for virtual currency, the term refers to a digital representation of value that is not government-issued legal tender. Unlike U.S. dollars and other government-issued currencies, virtual currencies do not necessarily have a physical coin or bill associated with their circulation. While virtual currencies can function as a unit of account, store of value, and medium of exchange, they are not widely used or accepted. Some virtual currencies can only be used within virtual economies (for example, within online role-playing games) and may not be readily exchanged for government-issued currencies such as U.S. dollars, euro, or yen. Other virtual currencies may be used to purchase goods and services in the real economy and can be converted into government-issued currencies through virtual currency exchanges. In previous work, we described the

[5]The Digital Economy Task Force was established in 2013 by Thomson Reuters (a multinational media and information firm) and the International Centre for Missing & Exploited Children to explore the benefits and risks of the emerging digital economy, including the use of virtual currency. This task force includes members from both the public and private sectors.

[6]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012) and *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, GAO-14-220 (Washington, D.C.: Feb. 14, 2014).

latter type of virtual currencies as "open flow."[7] Open-flow virtual currencies have received considerable attention from federal financial regulatory and law enforcement agencies, in part because these currencies interact with the real economy and because depository institutions (for example, banks and credit unions) may have business relationships with companies that exchange virtual currencies for government-issued currencies. Throughout the remainder of this report, we use the term virtual currencies to mean open-flow virtual currencies, unless otherwise stated.[8]

Virtual currency systems, which include protocols for conducting transactions in addition to digital representations of value, can either be centralized or decentralized. Centralized virtual currency systems have a single administering authority that issues the currency and has the authority to withdraw the currency from circulation. In addition, the administrating authority issues rules for use of the currency and maintains a central payment ledger. In contrast, decentralized virtual currency systems have no central administering authority. Validation and certification of transactions are performed by users of the system and therefore do not require a third party to perform intermediation activities.

A prominent example of a decentralized virtual currency system is bitcoin. Bitcoin was developed in 2009 by an unidentified programmer or programmers using the name Satoshi Nakamoto. According to industry stakeholders, bitcoin is the most widely circulated decentralized virtual currency. The bitcoin computer protocol permits the storage of unique digital representations of value (bitcoins) and facilitates the assignment of bitcoins from one user to another through a peer-to-peer, Internet-based

[7]GAO-13-516. In that report we described "closed-flow" virtual currencies as those that can be used only within a game or virtual environment and cannot be cashed out for dollars or other government-issued currencies. We also described hybrid virtual currencies as those that have characteristics of both open- and closed-flow currencies—for example, such currencies can be used to buy real goods and services but are not exchangeable for government-issued currencies.

[8]Some stakeholders with whom we spoke said they preferred the term digital currency to virtual currency, due partly to the connotation that something which is virtual cannot be used in the real world. We use the term virtual currency to be consistent with terminology used in prior GAO work and in key federal guidance on participants in virtual currency systems.

network.[9] Each bitcoin is divisible to eight decimal places, enabling their use in any kind of transaction regardless of the value. Users' bitcoin balances are associated with bitcoin addresses (long strings of numbers and letters) that use principles of cryptography to help safeguard against inappropriate tampering with bitcoin transactions and balances.[10] When users transfer bitcoins, the recipient provides their bitcoin address to the sender, and the sender authorizes the transaction with their private key (essentially a secret code that proves the sender's control over their bitcoin address). Bitcoin transactions are irrevocable and do not require the sender or receiver to disclose their identities to each other or a third party. However, each transaction is registered in a public ledger called the "blockchain," which maintains the associated bitcoin addresses and transaction dates, times, and amounts. Users can define how much additional information they require of each other to conduct a transaction.

Because peer-to-peer bitcoin transactions do not require the disclosure of information about a user's identity, they give the participants some degree of anonymity. In addition, computer network communication can be encrypted and anonymized by software to further hide the identity of the parties in transactions.[11] However, the transactions are not completely anonymous because the time and amount of each transaction and the associated bitcoin addresses are permanently recorded in the blockchain. As a result, peer-to-peer bitcoin transactions are sometimes described as "pseudonymous." The anonymity of bitcoin is also limited by data analysis techniques that can potentially link bitcoin addresses to personal identities. For example, information about a customer's identity may be recorded when an individual exchanges dollars for bitcoins, and this information may be combined with data from the blockchain to determine

[9]A peer-to-peer network allows users to share data directly and conduct permitted activities without a central server.

[10]Cryptography is a branch of mathematics that is based on the transformation of data and can be used to provide security services such as confidentiality and authentication. Bitcoin and other virtual currencies that use cryptography are sometimes called cryptocurrencies.

[11]According to industry observers, examples of technologies used to increase the privacy of participants in virtual currency transactions include (1) anonymizing networks, which use a distributed network of computers to conceal the real Internet address of users, such as The Onion Router (TOR); (2) "tumblers" such as BitcoinBath and BitLaundry that combine payments from multiple users to obstruct identification through the blockchain; and (3) alternative virtual currencies such as Zerocoin and Anoncoin that aim to make transactions fully anonymous.

the identities of participants in bitcoin transactions. In addition, researchers have developed methods to determine identities of parties involved in some bitcoin transactions by analyzing clusters of transactions between specific addresses.[12]

Bitcoins are created and entered into circulation through a process called mining. Bitcoin miners download free software that they use to solve complex math problems. Solving these problems verifies the validity of bitcoin transactions by grouping several transactions into a block and mathematically proving that the transactions occurred and did not involve double spending of a bitcoin. On average, this process takes about 10 minutes. When a miner or group of miners (mining pools) solves a problem, the bitcoin network accepts the block of transactions as valid and creates new bitcoins and awards them to the successful miner or mining pool.[13] (For a diagram on how bitcoins enter into circulation through mining, how transactions are conducted, and how miners verify transactions, see app. I.) Over time, the computer processing power needed to mine new bitcoins has increased to the point where mining requires specialized computer hardware and has become increasingly consolidated into large mining pools.

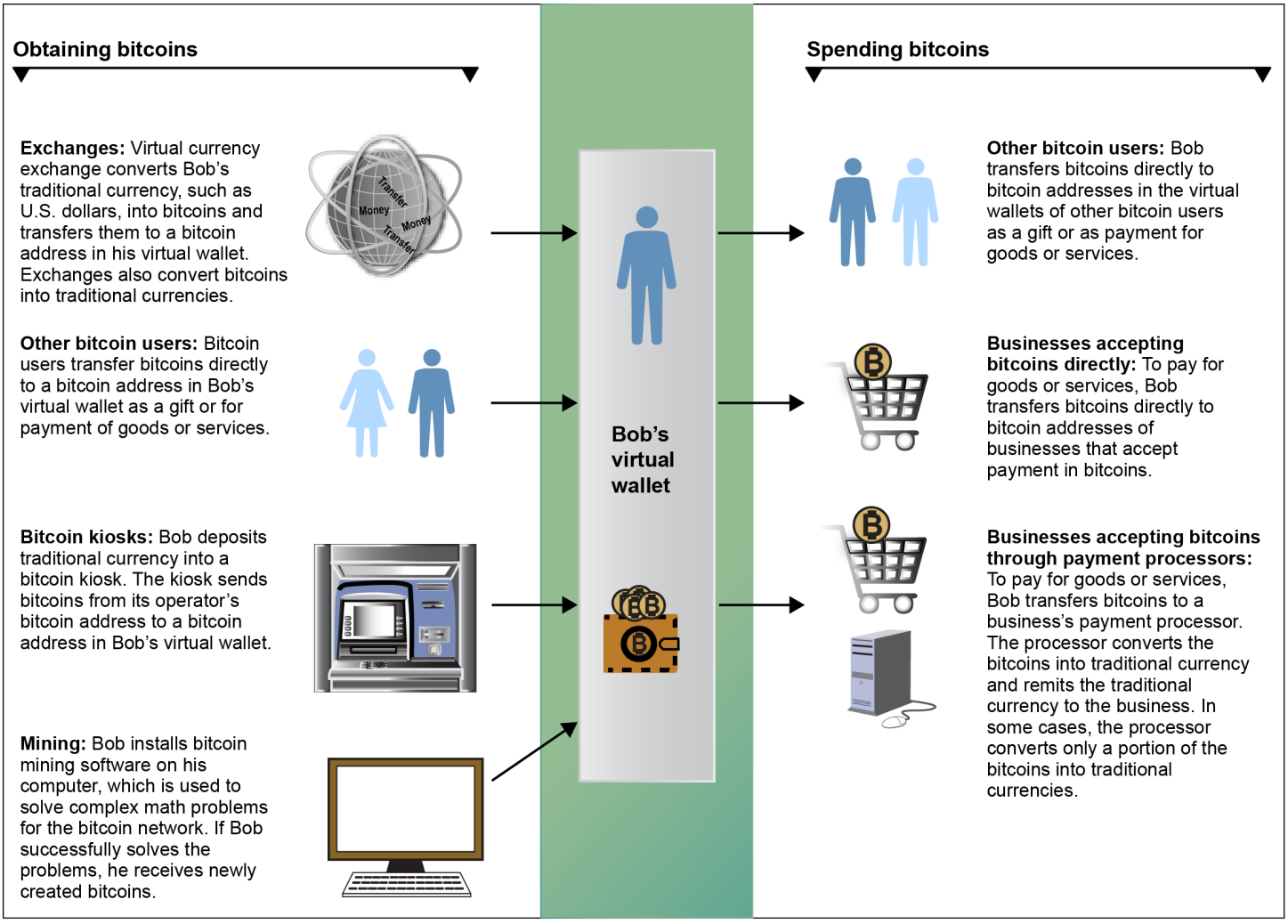
In addition to mining new bitcoins, users can also acquire bitcoins already in circulation by accepting bitcoins as gifts or payments for goods or services, purchasing them at bitcoin kiosks (sometimes referred to as bitcoin automated teller machines), or purchasing them on third-party exchanges. These exchanges allow users to exchange traditional currencies such as U.S. dollars for bitcoins, and exchange bitcoins back to traditional currencies. Individuals may store their bitcoins in a "virtual wallet" (a program that saves bitcoin addresses) on their computer or other data storage device, or use an online wallet service provided by an exchange or third-party virtual wallet provider. To spend their bitcoins, individuals can buy goods or services from other bitcoin users. They may also make purchases from online businesses that either accept bitcoins

[12]See Sarah Meiklejohn, et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *;Login:,* vol. 38 no. 6 (2013), available at https://www.usenix.org/system/files/login/articles/03_meiklejohn-online.pdf.

[13]By design, there will be a maximum of 21 million bitcoins in circulation once all bitcoins have been mined, which is projected to occur in the year 2140. Once all bitcoins have been mined, miners will be rewarded for solving the math problems that verify the validity of bitcoin transactions through fees rather than bitcoins.

directly or use third-party payment processors that take payments in bitcoins from buyers and provide businesses the payments in the form of a traditional currency or a combination of bitcoins and traditional currency. Figure 1 shows various ways that individuals can obtain and spend bitcoins.

Figure 1: Ways to Obtain and Spend Bitcoins



Source: GAO.

Due to limitations in available data, the size of the bitcoin market is unclear.[14] Nonetheless, some data exist that may provide some context for the size of this market:

- According to statistics from the bitcoin blockchain, as of March 31, 2014, approximately 12.6 million bitcoins were in circulation.[15]
- At exchange rates as of March 31, 2014 (about $458 per bitcoin), the total value of the approximately 12.6 million bitcoins in circulation was about $5.6 billion.[16] For perspective, the total amount of U.S. currency held by the public and in transaction deposits (mainly checking accounts) at depository institutions was about $2.7 trillion as of March 2014.[17]
- Bitcoin exchange rates against the U.S. dollar have changed dramatically over time (see fig. 2). According to one bitcoin price index, the price was about $13 per bitcoin in the beginning of January 2013 and rose to more than $1,100 by the beginning of December 2013. Prices subsequently fell to about $522 in mid-December 2013 and have fluctuated between roughly $450 and $950 since then.[18]
- From April 2013 through March 2014, the number of bitcoin transactions per day ranged from about 29,000 to 102,000.[19] In comparison, the Federal Reserve Banks processed an average of 44

[14]Given these limitations, we did not test the reliability of data, such as the data generated from the bitcoin network, but we are providing some figures to provide context for the possible size of the bitcoin market and other virtual currency markets.

[15]http://blockchain.info. (Accessed on Mar. 31, 2014.) Due to data limitations, it is difficult to calculate the velocity, or the rate at which bitcoins are spent, and the number of transactions between unique users in a given time period.

[16]For data on bitcoin price, see https://www.coindesk.com. (Accessed on Apr. 1, 2014.) For data on the total value and number of bitcoins in circulation, see https://blockchain.info. (Accessed on Mar. 31, 2014.)

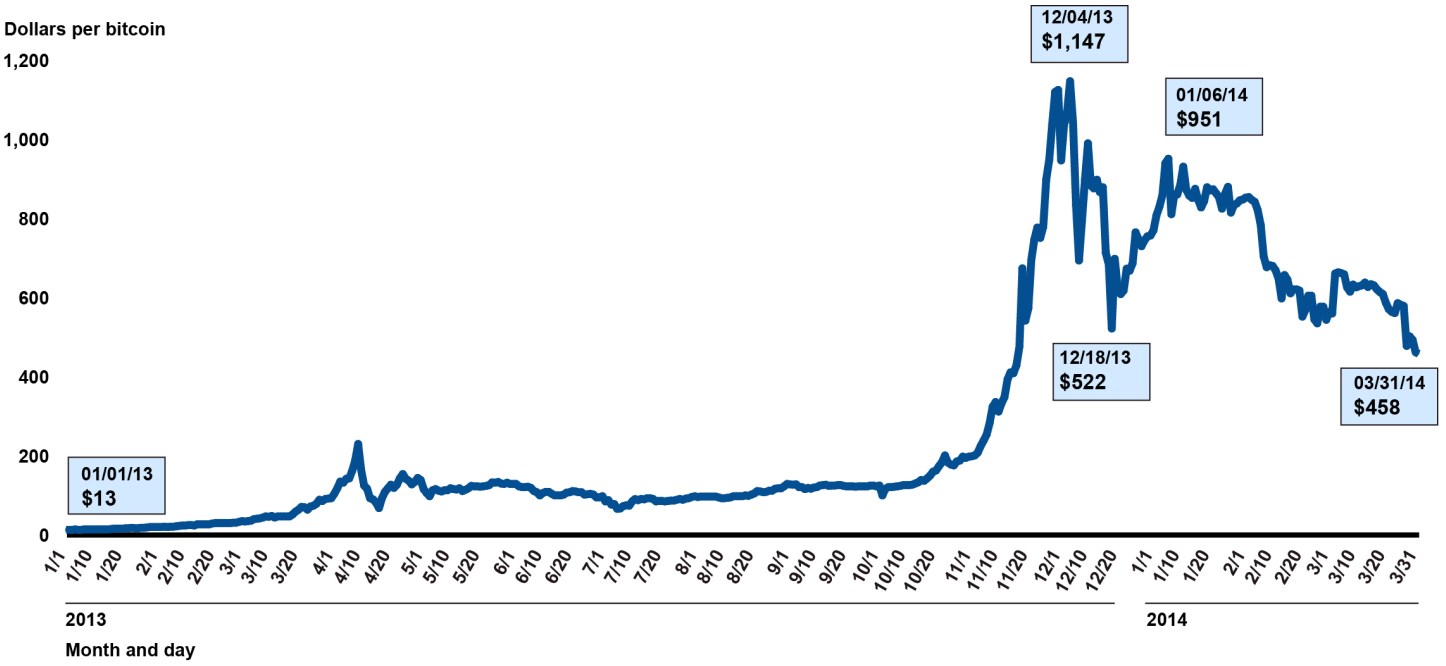
[17]See Federal Reserve Statistical Release H.6 “Money Stock Measures” (Apr. 10, 2014) at http://www.federalreserve.gov/releases/h6/current/H6.pdf.

[18]https://www.coindesk.com. (Accessed on Apr.1, 2014.) This index is a composite price calculated as the simple average of bitcoin prices across leading global exchanges that meet certain criteria.

[19]https://blockchain.info. (Accessed on Apr. 1, 2014.)

million commercial Automated Clearing House (a traditional payment processor) transactions per day in 2013.[20]

Figure 2: Bitcoin Price Index in U.S. Dollars, January 1, 2013 through March 31, 2014



Source: GAO analysis of data from http://www.coindesk.com/price/ (accessed on Apr. 1, 2014).

Note: The index is a composite price calculated as the simple average of bitcoin prices across leading global exchanges that meet certain criteria. The values are expressed in current U.S. dollars.

While bitcoin is the most widely used virtual currency, numerous others have been created. For example, dozens of decentralized virtual currencies are based on the bitcoin protocol such as Litecoin, Auroracoin, Peercoin, and Dogecoin. Similar to the bitcoin market, the size of the market for these virtual currencies is unclear. However, as of March 31, 2014, the total reported value of each of these currencies was less than $400 million (ranging from about $33 million for Dogecoin to about $346 million for Litecoin).[21] Other virtual currencies that have been created are

[20]Federal Reserve. See http://www.federalreserve.gov/paymentsystems/fedach_yearlycomm.htm. (Accessed on Apr. 1, 2014.)

[21]https://coinmarketcap.com. (Accessed on Apr. 1, 2014.)

not based on the bitcoin protocol. One of the more prominent examples is XRP, which is used within a decentralized payment system called Ripple. Ripple allows users to make peer-to-peer transfers in any currency. A key function of XRP is to facilitate the conversion from one currency to another. For example, if a direct conversion between Mexican pesos and Thai baht is not available, the pesos can be exchanged for XRP, and then the XRP for baht. As of March 31, 2014, the total value of XRP was $878 million.[22]

Virtual currencies have drawn attention from federal agencies with responsibilities for protecting the U.S. financial system and its participants and investigating financial crimes. These include, but are not limited to, CFPB, CFTC, DHS, DOJ, SEC, Treasury, and the prudential banking regulators. The prudential banking regulators are the FDIC, Federal Reserve, NCUA, and OCC. Within Treasury, FinCEN has a particular interest in the emergence of virtual currencies because of concerns about the use of these currencies for money laundering and FinCEN's role in combating such activity.[23] Additionally, because virtual currencies (like government-issued currencies) can play a role in a range of financial and other crimes, including cross-border criminal activity, key components of DOJ and DHS have an interest in how virtual currencies are used. Relevant DOJ components include the Criminal Division (which oversees the Computer Crime and Intellectual Property Section and the Asset Forfeiture and Money Laundering Section), the FBI, and the Offices of the U.S. Attorneys (U.S. Attorneys). Relevant DHS components include the Secret Service and ICE-HSI.

[22]https://coinmarketcap.com.(Accessed on Apr. 1, 2014.)

[23]Money laundering is the process of disguising or concealing the source of funds acquired illicitly to make the acquisition appear legitimate.

Federal Agencies Face Emerging Challenges in Carrying Out Responsibilities Related to the Use of Virtual Currencies

While federal agencies' responsibilities with respect to virtual currency are still being clarified, some virtual currency activities and products have implications for the responsibilities of federal financial regulatory and law enforcement agencies. Virtual currencies have presented these agencies with emerging challenges as they carry out their different responsibilities. These challenges stem partly from certain characteristics of virtual currency systems, such as the higher degree of anonymity they provide compared with traditional payment systems and the ease with which they can be accessed globally to make payments and transfer funds across borders.

Some Virtual Currency Activities and Products May Have Implications for Federal Agencies' Responsibilities

Although virtual currencies are not government-issued and do not currently pass through U.S. banks, some activities and products that involve virtual currencies have implications for the responsibilities of federal financial regulatory and law enforcement agencies. These activities and products encompass both legitimate and illegitimate uses of virtual currencies. Examples of legitimate uses include buying virtual currencies and registered virtual-currency-denominated investment products. Examples of illegitimate uses include money laundering and purchasing illegal goods and services using virtual currencies.

FinCEN

FinCEN administers BSA and its implementing regulations.[24] The goal of BSA is to prevent financial institutions from being used as intermediaries for the transfer or deposit of money derived from criminal activity and to provide a paper trail to assist law enforcement agencies in their money laundering investigations. To the extent that entities engaged in money transmission conduct virtual currency transactions with U.S. customers or become customers of a U.S. financial institution, FinCEN has

[24]Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829(b), 1951-1959; 31 U.S.C. §§ 5311-5330); 31 C.F.R. chap. X. In 1994, the Secretary of the Treasury delegated overall authority for enforcement of, and compliance with, BSA and its implementing regulations related to money laundering to the Director of FinCEN. In the same year, the Secretary also delegated BSA examination authority to the prudential banking regulators. 31 C.F.R. § 1010.810(b)(1)-(5).

responsibilities for helping ensure that these entities comply with BSA and anti-money-laundering regulations.[25]

FinCEN regulations set forth requirements for money services businesses, which include financial institutions and other entities engaged in money transmission.[26] FinCEN guidance states that the agency's regulations regarding money services businesses apply to virtual currency exchangers and administrators.[27] FinCEN applies its regulations to "convertible virtual currency," which either has an equivalent value in real currency or acts as a substitute for real currency. FinCEN regulations require money services businesses to assess their exposure to money laundering and terrorist financing and establish risk mitigation plans in the form of anti-money-laundering programs.[28] Additionally, money services businesses are required to maintain transaction records. For example, for money transfers that are $3,000 or more, money services businesses must obtain information on the transmitter, the recipient, and the transaction itself, and pass on such information to other intermediary financial institutions in any subsequent fund transmissions. Money

[25]FinCEN shares this responsibility with IRS, to which FinCEN has delegated examination authority for money services businesses. See 31 C.F.R. § 1010. 810(b)(8). IRS activities were outside the scope of our review. FinCEN has also delegated examination authority for BSA compliance to a number of other federal agencies, including the prudential banking regulators, CFTC, and SEC. See 31 C.F.R. § 1010.810(b). These agencies can also use their independent authorities to examine entities under their supervision for compliance with applicable BSA and anti-money-laundering requirements and regulations.

[26]Under 31 C.F.R. § 1010.100(ff)(1)-(7), money services businesses are generally defined as any of the following: (1) currency dealer or exchanger, (2) check casher, (3) issuer or seller of traveler's checks or money orders, (4) provider or seller of prepaid access, (5) money transmitter, and (6) the U.S. Postal Service. FinCEN's regulations define a money transmitter as a person that provides money transmission services, or any other person engaged in the transfer of funds. 31 C.F.R. § 1010.100(ff)(5)(i).The term money transmission services means the "acceptance of currency, funds, or other value that substitutes for currency to another location or person by any means." Id.

[27] FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, March 18, 2013. FinCEN defines an exchanger as a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. *Id*. FinCEN defines an administrator as a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. *Id.* An administrator or exchanger that (1) accepts and transmits a convertible virtual currency, or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations.

[28]31 C.F.R. § 1022.210, subpart C.

services businesses are also required to monitor transactions and file reports on large currency transactions and suspicious activities. In addition, certain financial institutions must establish a written customer identification program that includes procedures for obtaining minimum identification information from customers who open an account, such as date of birth, a government identification number, and physical address.[29] Further, financial institutions must file currency transaction reports on customer cash transactions exceeding $10,000 that include information about the account owner's identity and occupation.[30]

FinCEN also supports the investigative and prosecutive efforts of multiple federal and state law enforcement agencies through its administration of the financial transaction reporting and recordkeeping requirements mandated or authorized under BSA. In addition, FinCEN has the authority to take enforcement actions, such as assessing civil money penalties, against financial institutions, including money services businesses, that violate BSA requirements.

Prudential Banking Regulators

The prudential banking regulators—FDIC, Federal Reserve, NCUA, and OCC—provide oversight of depository institutions' compliance with BSA and anti-money-laundering requirements. Therefore, these regulators are responsible for providing guidance and oversight to help ensure that depository institutions that have opened accounts for virtual currency exchanges or other money services businesses have adequate anti-money-laundering controls for those accounts.[31] In April 2005, FinCEN and the prudential banking regulators issued joint guidance to banking organizations (depository institutions and bank holding companies) to clarify BSA requirements with respect to money services businesses and to set forth the minimum steps that banking organizations should take

[29]31 C.F.R. § 1020.220(a)(2)(i). Under the USA PATRIOT Act, financial institutions also must implement appropriate, specific, and, where necessary, enhanced, due diligence for correspondent accounts and private banking accounts established in the United States for non-U.S. persons. 31 U.S.C. § 5318(i).

[30]31 U.S.C. § 5313(a); 31 C.F.R. § 1010.311.

[31]In addition, officials from the prudential banking regulators either stated or acknowledged that they would have authority to regulate a supervised entity that issued virtual currency, or cleared or settled transactions related to virtual currency.

when providing banking services to these businesses.[32] As part of safety and soundness or targeted BSA compliance examinations of depository institutions, the prudential banking regulators assess compliance with BSA and related anti-money-laundering requirements using procedures that are consistent with their overall risk-focused examination approach.[33] In examining depository institutions for BSA compliance, the regulators review whether depository institutions (1) have developed anti-money-laundering programs and procedures to detect and report unusual or suspicious activities possibly related to money laundering; and (2) comply with the technical recordkeeping and reporting requirements of BSA.[34] While most cases of BSA noncompliance are corrected within the examination framework, regulators can take a range of supervisory actions, including formal enforcement actions, against the entities they supervise for violations of BSA and anti-money-laundering requirements. These formal enforcement actions can include imposing civil money penalties and initiating cease-and-desist proceedings.[35]

Consumer Financial Protection Bureau

CFPB is an independent entity within the Federal Reserve that has broad consumer protection responsibilities over an array of consumer financial products and services, including taking deposits and transferring money. CFPB is responsible for enforcing federal consumer protection laws, and it is the primary consumer protection supervisor over many of the

[32]FinCEN, *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States*, April 26, 2005. FinCEN concurrently issued guidance to money services businesses that identified and explained the types of information and documentation that money services businesses were expected to have and provide to banking organizations. Bank holding companies are companies that own or control one or more banks. In the United States, most banks insured by FDIC are owned or controlled by a bank holding company.

[33]Under the risk-focused approach, those activities judged to pose the highest risk to an institution are to receive the most scrutiny by examiners.

[34]See 12 U.S.C. § 1786(q), § 1818(s) (federal banking agencies must promulgate regulations requiring insured depository institutions and credit unions to establish procedures regarding BSA compliance; regulators' examinations must include review of BSA compliance procedures); see also procedures for monitoring BSA compliance: 12 C.F.R. § 208.63 (Federal Reserve), 12 C.F.R. § 326.8 (FDIC), 12 C.F.R. § 748.2 (NCUA), and 12.C.F.R. § 21.21 (OCC).

[35]A civil money penalty is a punitive fine assessed for the violation of a law or regulation or for other misconduct. A cease-and-desist proceeding is a formal process that may result in an order that a party halt certain activities or practices; the order may also require the party to take affirmative action to correct the conditions resulting from the practices. See 12 U.S.C. § 1786(e), § 1818(b).

institutions that offer consumer financial products and services. CFPB also has authority to issue and revise regulations that implement federal consumer financial protection laws, including the Electronic Fund Transfer Act[36] and title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).[37] CFPB officials stated that they are reviewing how these responsibilities are implicated by consumer use (or potential consumer use) of virtual currencies.

Other relevant CFPB responsibilities concerning virtual currencies include accepting and handling consumer complaints, promoting financial education, researching consumer behavior, and monitoring financial markets for new risks to consumers. For example, under authorities provided by the Dodd-Frank Act, CFPB maintains a Consumer Complaint Database and helps monitor and assess risks to consumers in the offering or provision of consumer financial products or services.[38] CFPB also issues consumer advisories to promote clarity, transparency, and fairness in consumer financial markets.

Securities and Exchange Commission

SEC regulates the securities markets—including participants such as securities exchanges, broker-dealers, investment companies, and investment advisers—and takes enforcement actions against individuals and companies for violations of federal securities laws. SEC's mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. Virtual currencies may have implications for a number of SEC responsibilities. For example, SEC has enforcement

[36]Pub. L. No. 90-321, 92 Stat. 3728 (1978) (codified as amended at 15 U.S.C. §§ 1693-1693r). CFPB issues and enforces Regulation E, which implements the Electronic Fund Transfer Act (EFTA). EFTA establishes basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services.

[37]Pub. L. No. 111-203, § 1021(c)(5), 124 Stat. 1376, 1980 (2010) (codified at 12 U.S.C. § 5511(c)(5)). For example, section 1032(a) of the Dodd-Frank Act confers authority on CFPB "to prescribe rules to ensure that the features of any consumer financial product or service, both initially and over the term of the product or service, are fully, accurately, and effectively disclosed to consumers in a manner that permits consumers to understand the costs, benefits, and risks associated with the product or service, in light of the facts and circumstances." 12 U.S.C. § 5532(a). In prescribing such disclosure rules, section 1032 requires the Bureau to "consider available evidence about consumer awareness, understanding of, and responses to disclosures or communications about the risks, costs, and benefits of consumer financial products or services." 12 U.S.C. § 5532(c).

[38]Pub. L. No. 111-203, § 1013(b)(3), § 1021(c), 124 Stat. 1376, 1969, 1980 (2010) (codified at 12 U.S.C. §§ 5493(b)(3), 5511(c)).

authority for violations of federal securities laws prohibiting fraud by any person in the purchase, offer, or sale of securities. SEC enforcement extends to virtual-currency-related securities transactions. Additionally, when companies offer and sell securities (including virtual-currency-related securities), they are subject to SEC requirements to either register the offering with SEC or qualify for a registration exemption. SEC reviews registration statements to ensure that potential investors receive adequate information about the issuer, the security, and the offering. Further, if a registered national securities exchange wanted to list a virtual-currency-related security, it could only do so if the listing complied with the exchange's existing rules or the exchange had filed a proposed rule change with SEC to permit the listing.

Virtual currencies may also have implications for other SEC responsibilities, as the following examples illustrate:

- SEC has examination authority for entities it regulates, including registered broker-dealers, to ensure compliance with federal securities laws, SEC rules and regulations, and BSA requirements. According to SEC officials, if a broker-dealer were to accept payments in virtual currencies from customers, this could raise potential anti-money-laundering issues that the broker-dealer would have to account for.
- SEC also regulates and has examination authority over investment advisers subject to its jurisdiction.[39] Under the Investment Advisers Act of 1940, investment advisers are fiduciaries.[40] To the extent that an investment adviser recommends virtual currencies or virtual-currency-related securities, the investment adviser's federal fiduciary duty would govern this conduct.
- If registered broker-dealers held virtual currencies for their own account or an account of a customer, SEC would have to determine how to treat the virtual currencies for purposes of its broker-dealer financial responsibility rules, including the net capital rule.[41]

[39]15 U.S.C. §§ 80b-2(a)(11), 80b-11(g)-(h).

[40]See 15 U.S.C. § 80b-6(1)-(2); *SEC v. Capital Gains Research Bureau, Inc.,* et al., 375 U.S. 180 (1963).

[41]17 C.F.R. § 240.15c3-1. SEC's net capital rule requires all broker-dealers to maintain a minimum level of net capital consisting of highly liquid assets. Assets that are not liquid are deducted in full when computing net capital.

Commodity Futures Trading Commission

CFTC has the authority to regulate financial derivative products and their markets, including commodity futures and options.[42] In addition, CFTC investigates and prosecutes alleged violations of the Commodity Exchange Act and related regulations.[43] CFTC's mission is to protect market users and the public from fraud, manipulation, abusive practices, and systemic risk related to derivatives subject to the Commodity Exchange Act. CFTC's responsibilities with respect to virtual currencies depend partly on whether bitcoin or other virtual currencies meet the definition of a commodity under the Commodity Exchange Act.[44] CFTC officials said the agency would not make a formal determination on this issue until market circumstances require one. According to CFTC, such circumstances could include virtual-currency derivatives emerging or being offered in the United States or CFTC becoming aware of the existence of fraud or manipulative schemes involving virtual currencies. The officials said that if prospective derivatives that are backed by or denominated in virtual currencies that CFTC determines to be commodities emerge, CFTC's regulatory authorities would apply to those derivatives just as they would for any other derivative product subject to CFTC's jurisdiction. To carry out its regulatory responsibilities, CFTC would, among other things, evaluate the derivatives to ensure they were not susceptible to manipulation, review applications for new exchanges wishing to offer such derivatives, and examine exchanges offering these derivatives to ensure compliance with the applicable commodity exchange laws.

Similar to SEC, CFTC has examination authority for BSA compliance—in this case directed at futures commission merchants and other futures market intermediaries—and acceptance of virtual currency payments by

[42]7 U.S.C. § 2. Financial derivatives are financial instruments whose value is based on one or more underlying reference items. They are used to hedge risk or to exchange a floating rate of return for a fixed rate of return. In the virtual currency context, a derivative might be used to reduce exposure to volatility in virtual currency exchange rates.

[43]7 U.S.C. §§ 1-26; 17 C.F.R. chap. I.

[44]The Commodity Exchange Act defines a commodity as certain agricultural goods and "all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in." 7 U.S.C. § 1a(9).

these entities could raise BSA compliance concerns.[45] Like SEC, CFTC would also have to make determinations about the capital treatment of virtual currencies if these entities held virtual currencies for their own account or an account of a customer.

Departments of Homeland Security and Justice

Law enforcement agencies, including but not limited to DHS and DOJ component agencies and offices, have responsibilities to investigate a variety of federal crimes that may involve the use of virtual currencies and to support the prosecution of those who commit these crimes. Like traditional currencies, virtual currencies can facilitate a range of criminal activities, including fraud schemes and the sale of illicit goods and services, that may fall under the purview of federal law enforcement agencies.

The emergence of virtual currencies has had particular significance for financial crimes. According to DOJ officials, the main law enforcement interests with respect to virtual currencies are to (1) deter and prosecute criminals who use virtual currency systems to launder money (that is, move or hide money that either facilitates or is derived from criminal or terrorist activities); and (2) investigate and prosecute virtual currency services that themselves violate money transmission and money laundering laws.[46] A number of DOJ and DHS components, including the FBI, ICE-HSI, and Secret Service, investigate financial crimes as part of their broader responsibilities. In addition, DOJ's Asset Forfeiture and Money Laundering Section prosecutes money laundering violations, and DOJ and DHS manage the seizure and forfeiture of assets that represent the proceeds of, or were used to facilitate, federal crimes. Key laws that may apply to the use of virtual currencies in financial crimes include BSA,

[45]Futures commission merchants are entities that solicit or accept orders for the purchase or sale of a commodity for future delivery on or subject to the rules of any exchange and that accept payment from or extend credit to those whose orders are accepted.

[46]One example would be a centralized virtual currency system that allowed users to make untraceable funds transfers.

as amended by Title III of the USA PATRIOT Act, and anti-money-laundering statutes.[47]

Additionally, because virtual currencies operate over the Internet, they have implications for agency components that investigate and prosecute computer crimes (also called cybercrimes). For example, DOJ's Computer Crime and Intellectual Property Section stated that virtual currencies can be attractive to entities that seek to facilitate or conduct computer crimes over the Internet, such as computer-based fraud and identity theft. The section's responsibilities include improving legal processes for obtaining electronic evidence and working with other law enforcement agencies in improving the technological and operational means for gathering and analyzing electronic evidence. The FBI, Secret Service, and ICE-HSI also investigate computer crimes.

Virtual Currencies Present Regulatory, Law Enforcement, and Consumer Protection Challenges

The emergence of virtual currencies presents challenges to federal agencies responsible for financial regulation, law enforcement, and consumer and investor protection. These challenges stem partly from certain characteristics of virtual currencies, such as the higher degree of anonymity they provide and the ease with which they can be sent across borders. In addition, the growing popularity of virtual currencies has highlighted both risks and benefits for agencies to consider in carrying out their responsibilities.

Greater Anonymity

As previously noted, some virtual currency systems may provide a higher degree of anonymity than traditional payment systems because they do not require the disclosure of personally identifiable information (that is, information that can be used to locate or identify an individual, such as names or Social Security numbers) to transfer funds from one party to another. When transferring funds in the amount of $3,000 or more between the bank accounts of two individuals, the banks involved are required by FinCEN regulations to obtain and keep the names and other

[47]Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1829(b), 1951-1959; 31 U.S.C. §§ 5311-5330); Pub. L. No. 107-56, tit. III, 115 Stat. 272, 296-342 (International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001) (codified at 31 U.S.C. §§ 5301-5318A) (to prevent, detect, and prosecute international money laundering); see also Money Laundering Suppression Act of 1994, Pub. L. No. 103-325, §§ 401-413, 108 Stat. 2160, 2243-2255 (codified at 31 U.S.C. § 5330 and scattered sections of U.S.C.) (requires money transmitting businesses to register with Treasury).

information of the individuals, as well as information on the transaction itself.[48] The customer identification information collected by the banks helps create a paper trail of financial transactions that law enforcement agencies can use to detect illegal activity, such as money laundering or terrorist financing, and to identify and apprehend criminals.[49] However, in a transfer between two individuals using bitcoins (or a similar type of decentralized virtual currency) no personally identifiable information is necessarily disclosed either to the two individuals or a third-party intermediary.[50] As a result, virtual currencies may be attractive to parties seeking to protect personally identifiable information, maintain financial privacy, buy or sell illicit goods and services, or move or conceal money obtained by illegal means. Further, virtual currency exchangers or administrators may be used to facilitate money laundering if they do not collect identifying information from customers and retain other transaction information. For these reasons, law enforcement and federal financial regulatory agencies have indicated that virtual currencies can create challenges for agencies in detecting unlawful actions and the entities that carry them out. For example, the FBI has noted that because bitcoin does not have a centralized entity to monitor and report suspicious activity and process legal requests such as subpoenas, law enforcement agencies face difficulty in detecting suspicious transactions using bitcoins and identifying parties involved in these transactions.

Cross-Jurisdictional Nature

Because they operate over the Internet, virtual currencies can be used globally to make payments and funds transfers across borders. In addition, according to agency officials, many of the entities that exchange traditional currencies for virtual currencies (or vice versa) are located outside of the United States. If these exchangers have customers located in the United States, they must comply with BSA and anti-money-laundering requirements. Due to the cross-jurisdictional nature of virtual

[48]31 C.F.R. § 1020.410.

[49]Financial institutions are also required to obtain customer information to satisfy "know-your-customer" or "customer due diligence" identification programs as part of their anti-money laundering obligations, and financial institutions must subject certain bank accounts held by non-U.S. persons to enhanced due diligence procedures. See 31 U.S.C. § 5318(i).

[50]However, in a virtual currency transfer between individuals through a third-party intermediary (such as a virtual currency exchange), personally identifiable information is required to be collected if the transaction is for $3,000 or more. This requirement became effective in 2011. We discuss this requirement in the next section of this report.

currency systems, federal financial regulatory and law enforcement agencies face challenges in enforcing these requirements and investigating and prosecuting transnational crimes that may involve virtual currencies. For example, law enforcement may have to rely upon cooperation from international partners to conduct investigations, make arrests, and seize criminal assets. Additionally, violators, victims, and witnesses may reside outside of the United States, and relevant customer and transaction records may be held by entities in different jurisdictions, making it difficult for law enforcement and financial regulators to access them. Further, virtual currency exchangers or administrators may operate out of countries that have weak legal and regulatory regimes or that are less willing to cooperate with U.S. law enforcement.

Balancing Risks and Benefits

Virtual currency industry stakeholders have noted that virtual currencies present both risks and benefits that federal agencies need to consider in regulating entities that may be associated with virtual-currency-related activities. As previously noted, the risks include the attractiveness of virtual currencies to those who may want to launder money or purchase illicit goods and services. Another emerging set of risks involves consumer and investor protection—in particular, whether consumers and investors understand the potential drawbacks of buying, holding, and using virtual currencies or investing in virtual-currency-based securities. Consumers may not be aware of certain characteristics and risks of virtual currencies, including the following:

- *Lack of bank involvement.* Virtual currency exchanges and wallet providers are not banks. If they go out of business, there may be no specific protections like deposit insurance to cover consumer losses.[51]
- *Stated limits on financial recourse.* Some virtual currency wallet providers purport to disclaim responsibility for consumer losses associated with unauthorized wallet access. In contrast, credit and debit card networks state that consumers have no liability for fraudulent use of accounts.
- *Volatile prices.* The prices of virtual currencies can change quickly and dramatically (as shown previously in fig. 2).

Additionally, an SEC official told us that virtual-currency-based securities may be attracting individuals who are younger and less experienced than typical investors. The official expressed concern that younger investors

[51]We discuss examples of such losses in the next section of this report.

may lack the sophistication to properly assess the risks of such investments and the financial resources to recover from losses on the investments, including losses resulting from fraud schemes.[52]

While virtual currencies present risks to consumers and investors, they also provide several potential benefits to consumers and business.

- *Cost and speed.* Decentralized virtual currency systems may, in some circumstances, provide lower transaction costs and be faster than traditional funds transfer systems because the transactions do not need to go through a third-party intermediary. The irrevocable feature of virtual currency payments may also contribute to lower transaction costs by eliminating the costs of consumer chargebacks.[53] Industry stakeholders have noted that cost and time savings may be especially significant for international remittances (personal funds immigrants send to their home countries), which sometimes involve sizeable fees and can take several days. In addition, industry stakeholders have indicated that the potentially lower costs of virtual currency transactions—for example, relative to credit and debit cards—may facilitate the use of micropayments (very small financial transactions) as a way of selling items such as online news articles, music, and smartphone applications.
- *Financial privacy.* To the extent that bitcoin (or other virtual currency) addresses are not publicly associated with a specific individual, peer-to-peer virtual currency transactions can provide a greater degree of financial privacy than transactions using traditional payment systems, because no personally identifiable information is exchanged.[54]
- *Access.* Because virtual currencies can be accessed anywhere over the Internet, they are a potential way to provide basic financial services to populations without access to traditional financial

[52]The next section of this report discusses an example of a fraud scheme involving a virtual-currency-based security.

[53]A chargeback is a payment reversal initiated by a consumer due, for example, to nondelivery of a purchased product.

[54]As previously noted, that privacy may be lost if a connection is established between a bitcoin address and its owner.

institutions, such as rural populations in developing countries.[55] However, the potential benefit hinges on access to the Internet, which these populations may not have, and may be offset by the lack of protections against losses noted previously.

Federal agency officials have acknowledged the need to consider both the risks and benefits of virtual currencies in carrying out their responsibilities. For example, the Director of FinCEN has testified that the emergence of virtual currencies has prompted consideration of vulnerabilities that these currencies create in the financial system and how illicit actors will take advantage of them. However, she also noted that innovation is an important part of the economy and that FinCEN needs to have regulation that mitigates concerns about illicit actors while minimizing regulatory burden. Similarly, the former Acting Assistant Attorney General for DOJ's Criminal Division has testified that law enforcement needs to be vigilant about the criminal misuse of virtual currency systems while recognizing that there are many legitimate users of those services. Balancing concerns about the illicit use of virtual currencies against the potential benefits of these technological innovations will likely be an ongoing challenge for federal agencies.

Agencies Have Taken Some Actions on Virtual Currencies, but Interagency Working Groups Have Not Focused on Consumer Risks

Federal financial regulators and law enforcement agencies have taken a number of actions related to the emergence of virtual currencies, including providing regulatory guidance, assessing anti-money-laundering compliance, and investigating crimes and violations that have been facilitated by the use of virtual currencies. However, interagency working groups addressing virtual currencies have not focused on consumer protection and have generally not included CFPB.

[55]Some industry observers have suggested that virtual currency system protocols may have applications beyond financial transactions. For example, just as the bitcoin protocol transfers and records ownership rights to currency, it could, in theory, be used to transfer and record ownership rights to stocks, among other things.

FinCEN Has Issued Rules, Guidance, and Administrative Rulings Regarding Virtual Currencies

FinCEN has taken a number of actions in recent years to establish and clarify requirements for participants in virtual currency systems. For example, in July 2011, FinCEN finalized a rule that modified the definitions of certain money services businesses.[56] Among other things, the rule states that persons who accept and transmit currency, funds, or "other value that substitutes for currency," are considered to be money transmitters.[57] Additionally, in March 2013, FinCEN issued guidance that clarified the applicability of BSA regulations to participants in certain virtual currency systems.[58] The FinCEN guidance classified virtual currency exchangers and administrators as money services businesses and, more specifically, as money transmitters.[59] The guidance also specified that virtual currency users are not money services businesses.[60] As a result, the guidance clarified that virtual currency exchangers and administrators must follow requirements to register with FinCEN as money transmitters; institute risk assessment procedures and anti-money-laundering program control measures; and implement certain recordkeeping, reporting, and transaction monitoring requirements, unless an exception to these requirements applies.[61] According to FinCEN officials, as of December 2013, approximately 40 virtual currency exchangers or administrators had registered with FinCEN.

[56] *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 Fed. Reg. 43585 (July 21, 2011).

[57] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[58] FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, March 18, 2013. This guidance addresses convertible virtual currency—that is, virtual currency which either has an equivalent value in real currency or acts as a substitute for real currency.

[59] According to FinCEN, virtual currency exchangers and administrators with U.S. customers must comply with BSA requirements, such as instituting anti-money-laundering controls, even if they are based outside of the United States.

[60] FinCEN's guidance defines a virtual currency user as "a person who obtains convertible virtual currency and uses it to purchase real or virtual goods or services on the user's own behalf." Although a user is not considered to be a money transmitter, FinCEN warns that a user's activities must still comply with other federal and state laws and regulations.

[61] Most states also regulate money services businesses and some have taken steps to address virtual currencies. For example, New York is developing licensing and regulatory requirements specific to virtual currency exchanges and Texas has issued a memorandum describing how current licensing requirements apply to virtual currency exchanges. FinCEN coordinates with its state counterparts to encourage application of FinCEN's guidance on virtual currencies as part of this process.

In 2014, in response to questions from industry stakeholders, FinCEN issued administrative rulings to clarify the types of participants to which the March 2013 guidance applies.[62] In January 2014, FinCEN issued rulings stating that the way in which a virtual currency is obtained is not material, but the way in which a person or corporation uses the virtual currency is. As a result, the rulings specify that two kinds of users are not considered money transmitters subject to FinCEN's regulations: miners who use and convert virtual currencies exclusively for their own purposes and companies that invest in virtual currencies exclusively as an investment for their own account.[63] However, the rulings specify that these two kinds of users may no longer be exempt from FinCEN's money transmitter requirements if they conduct their activities as a business service for others. The rulings also note that transfers of virtual currencies from these types of users to third parties should be closely scrutinized because they may constitute money transmission. In April 2014, FinCEN issued another administrative ruling, which states that companies that rent computer systems for mining virtual currencies are not considered money transmitters subject to FinCEN's regulations.[64]

FinCEN has also taken additional steps to help ensure that companies required to register as money services businesses under FinCEN's March 2013 virtual currency guidance have done so. According to FinCEN officials, FinCEN has responded to letters from companies seeking clarification about their requirements. Also, officials told us that FinCEN has proactively informed other companies that they should register as money services businesses.

[62]FinCEN, *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001, January 30, 2014, and FinCEN, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002, January 30, 2014.

[63]For example, a company that purchases and sells virtual currencies whenever such purchases and sales make investment sense according to the company's business plan is acting as a virtual currency user, not a virtual currency exchange.

[64]FinCEN, *Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currencies,* FIN-2014-R007, April 29, 2014.

Some Financial Regulators Have Taken Actions Concerning Anti-Money-Laundering and Securities Law Compliance

As part of their oversight activities, NCUA and SEC have addressed situations involving virtual currencies, and other federal financial regulators have had internal discussions regarding virtual currencies. NCUA has had two supervisory situations in which credit unions were involved with activity related to virtual currencies. These situations emerged after reviews of credit unions found that their anti-money-laundering and antifraud measures needed to be revised in light of activity involving virtual currency exchanges.

- In 2013, NCUA issued a preliminary warning letter to a federal credit union that provided account services to money services businesses that also served as bitcoin exchanges. The warning letter was based on various conditions that NCUA determined could undermine the credit union's stability. For example, the credit union did not have adequate anti-money-laundering controls in place for its money services business accounts. Further, the letter stated that the credit union should not have served money services businesses that were not part of the credit union's strategic plan, and that serving these businesses was not consistent with the credit union's charter, which called for serving the local community. The warning letter required the credit union to immediately cease all transactions with these money services business accounts and establish an appropriate BSA and anti-money-laundering infrastructure. As a result, the credit union ceased such activity and strengthened its BSA and anti-money-laundering compliance program.
- In 2012, NCUA provided support to a state regulator's review of a credit union's commercial customer. The state regulator found that this commercial customer was a payment processor—that is, a payment network that allows any business or person to send, request, and accept money—that had customers that were bitcoin exchanges. According to NCUA, the state regulator worked with the credit union to ensure that its BSA compliance program was adequate to monitor and address the risks associated with payment processors that serve bitcoin exchanges. The state regulator also worked to ensure that the payment processor's risk management practices included sufficient antifraud and anti-money-laundering measures. The payment processor subsequently suspended all accounts that served virtual currency exchanges.

In addition, SEC has taken enforcement action against an individual and entity that are alleged to have defrauded investors through a bitcoin-

denominated Ponzi scheme.[65] The agency has also issued related investor alerts, has begun to review a registration statement from an entity that wants to offer virtual-currency-related securities, and is monitoring for potential securities law violations related to virtual currencies.

- In July 2013, SEC charged an individual and his company, Bitcoin Savings and Trust, with offering and selling securities in violation of the antifraud and registration provisions of securities laws.[66] Specifically, SEC alleges that the founder and operator defrauded investors through a bitcoin-denominated Ponzi scheme. The founder and operator allegedly promised investors up to 7 percent weekly interest. However, he allegedly used bitcoins from new investors to make purported interest payments and cover investor withdrawals on outstanding trust investments, diverted investors' bitcoins for day trading in his personal account on a bitcoin currency exchange, and exchanged investors' bitcoins for U.S. dollars to pay for personal expenses. SEC also alleges that Bitcoin Savings and Trust raised at least 700,000 bitcoins in investor funds, which amounted to more than $4.5 million based on the average price of bitcoin in 2011 and 2012 when the investments were offered and sold. This case was still unresolved as of April 14, 2014.
- SEC's Office of Investor Education and Advocacy has issued two investor alerts on virtual currencies.[67] The first alert, issued in July 2013, warned about fraudulent investment schemes that may involve bitcoin and other virtual currencies.[68] The second alert, issued in May

[65]A Ponzi scheme is a type of investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors.

[66]*Securities and Exchange Commission v. Shavers*, No. 413-CV-416 (E.D. Texas Aug. 6, 2013).

[67]In addition, in March 2014, the Financial Industry Regulatory Authority, a self-regulatory organization for the securities industry, issued an investor alert about the risks of buying, using, and speculating in virtual currencies and the potential for related scams. See http://www.finra.org/Investors/ProtectYourself/InvestorAlerts/FraudsAndScams/P456458. Also, in April 2014, the North American Securities Administrators Association issued an investor advisory on virtual currencies, related investment risks, and the types of investments that might involve virtual currencies. See http://www.nasaa.org/30631/informed-investor-advisory-virtual-currency.

[68]http://www.investor.gov/news-alerts/investor-alerts/investor-alert-ponzi-schemes-using-virtual-currencies.

2014, addressed fraud and other investment risks related to virtual currencies.[69]

- SEC staff have begun to review a registration statement from a company that wants to conduct a public offering of virtual-currency-related securities and has received notice of a company offering a private virtual-currency-related security, relying upon an exemption from registration. In July 2013, the Winklevoss Bitcoin Trust filed a registration statement for an initial public offering of its securities. The Trust is structured similarly to an exchange-traded fund and will hold bitcoins as its only assets.[70] The Trust filed amended registration statements in October 2013 and February 2014, but the registration statement remains pending as of April 14, 2014, meaning that the Trust is not yet permitted to sell its securities in a public offering. Also, in October 2013, Bitcoin Investment Trust, a bitcoin-denominated pooled investment fund affiliated with SecondMarket, Inc. and available only to accredited investors, filed a notice with SEC indicating that it had sold securities in an exempt offering in reliance on Rule 506(c) of the Securities Act.[71] Rule 506(c) allows an issuer to raise an unlimited amount of money, but imposes restrictions on who can invest in the offering and requires the issuer to take reasonable steps to verify that those investing are accredited investors.[72]
- SEC staff are also monitoring the Internet and other sources, such as referrals from other agencies, for potential securities law violations involving bitcoin and other virtual currencies.

[69]http://www.investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments.

[70]Exchange-traded funds are commonly structured as open-end investment companies and offer investors a proportionate share in a pool of stocks, bonds, and other assets.

[71]Rule 506(c) is one of the exemptive rules under Regulation D that allow some businesses to offer and sell their securities without having to register the offer and sale of securities with SEC. Regulation D is designed to (1) simplify the previously existing rules and regulations, (2) eliminate any unnecessary restrictions that those rules and regulations place on small business issuers, and (3) achieve uniformity between state and federal exemptions to facilitate capital formation consistent with protecting investors.

[72]17 C.F.R. § 230.506(c). Accredited investors include, among others, individuals whose net worth is more than $1 million (not including the value of their primary residence) or whose individual income exceeds at least $200,000 for the most recent 2 years (or joint income with a spouse exceeding $300,000 for those years) and a reasonable expectation of the same income level in the current year. It also includes certain types of entities, such as insurance companies, banks, and corporations with assets exceeding $5 million. 17 C.F.R. § 230.501(a).

Further, all of the federal financial regulatory agencies we interviewed have had internal discussions on how virtual currencies work and what implications the emergence of virtual currencies might have for their responsibilities. While agencies generally told us that their conversations have been informal and ad hoc, some efforts have been more organized:

- In 2013, the Federal Reserve took several steps to share information on virtual currencies among the Board of Governors and the 12 Federal Reserve Banks. Among other things, the Board of Governors' BSA and anti-money-laundering specialist conference included a session focused on FinCEN's virtual currency guidance and recent law enforcement actions. The Board of Governors also circulated general information about virtual currencies within the Federal Reserve System to use in answering questions from media and the public about virtual currencies and federal financial regulatory actions to date.
- In 2013, SEC formed an internal Digital Currency Working Group, which aims to foster information sharing internally and externally. According to SEC, the working group consists of approximately 50 members from among SEC's divisions and offices.
- In 2012, FinCEN held three internal information-sharing events on virtual currencies. These events covered issues including how virtual currencies compare to traditional currencies and risks related to emerging payment systems such as virtual currencies.

Law Enforcement Agencies Have Taken Actions against Parties Alleged to Have Used Virtual Currencies to Facilitate Crimes

Law enforcement agencies have taken actions against parties involved in the illicit use of virtual currencies to facilitate crimes. These parties have included administrators and users of centralized virtual currency systems designed to facilitate money laundering or other crimes, parties who have used virtual currencies to buy or sell illicit goods and services online, and virtual currency exchanges and online payment processors operating without the proper licenses.

- In 2013 and 2014, law enforcement agencies took actions against Silk Road, a black market website that allegedly accepted bitcoin as the sole payment method for the purchase of illegal goods and services. The website contained over 13,000 listings for controlled substances as well as listings for malicious software programs, pirated media content, fake passports, and computer hacking services (see fig.3). The FBI; Drug Enforcement Administration (DEA); IRS; ICE-HSI; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Secret Service; the U.S. Marshals Service; and Treasury's Office of Foreign Assets Control investigated the case together, along with officials from

New York as well as Australia, Iceland, Ireland, and France. In September and October 2013, law enforcement shut down the Silk Road website and seized approximately 174,000 bitcoins, which the FBI reported were worth approximately $34 million at the time of seizure.[73] In February 2014, DOJ indicted Silk Road's alleged owner and operator on charges including narcotics conspiracy, engaging in a continuing criminal enterprise, conspiracy to commit computer hacking, and money laundering conspiracy.

- In May 2013, law enforcement agencies seized the accounts of a U.S.-based subsidiary of Mt. Gox, a now-defunct Tokyo-based virtual currency exchange with users from multiple countries including the United States, on the basis that the subsidiary was operating as an unlicensed money services business. The seizure included U.S. bank accounts of Mt. Gox that were held by a private bank and Dwolla, an online payment processor that allegedly allowed users to buy and sell bitcoins on Mt. Gox. According to ICE-HSI, Mt. Gox had moved funds into numerous online black markets, the bulk of which were associated with the illicit purchase of drugs, firearms, and child pornography. At the direction of the U.S. Attorney's office, ICE-HSI ordered Dwolla to stop all payments to Mt. Gox and seized $5.1 million from the Mt. Gox subsidiary's U.S. accounts.

- Also in May 2013, law enforcement agencies shut down Liberty Reserve, a centralized virtual currency system that was allegedly designed and frequently used to facilitate money laundering and had its own virtual currency. Secret Service, ICE-HSI, and IRS investigated the case together, along with officials from 16 other countries. To shut down the site, FinCEN identified Liberty Reserve as a financial institution of primary money laundering concern under section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.[74] DOJ then charged Liberty Reserve with operating an unlicensed money transmission business and with money laundering for facilitating the movement of more than $6 billion

[73]As of March 31, 2014, these bitcoins were worth about $80 million, according to bitcoin prices from https://www.coindesk.com.

[74]31 U.S.C. § 5318A. Section 311 of the USA PATRIOT Act grants the Secretary of the Treasury the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transaction, or type of account is of "primary money laundering concern," to require domestic financial institutions and financial agencies to take certain "special measures" to address the primary money laundering concern.

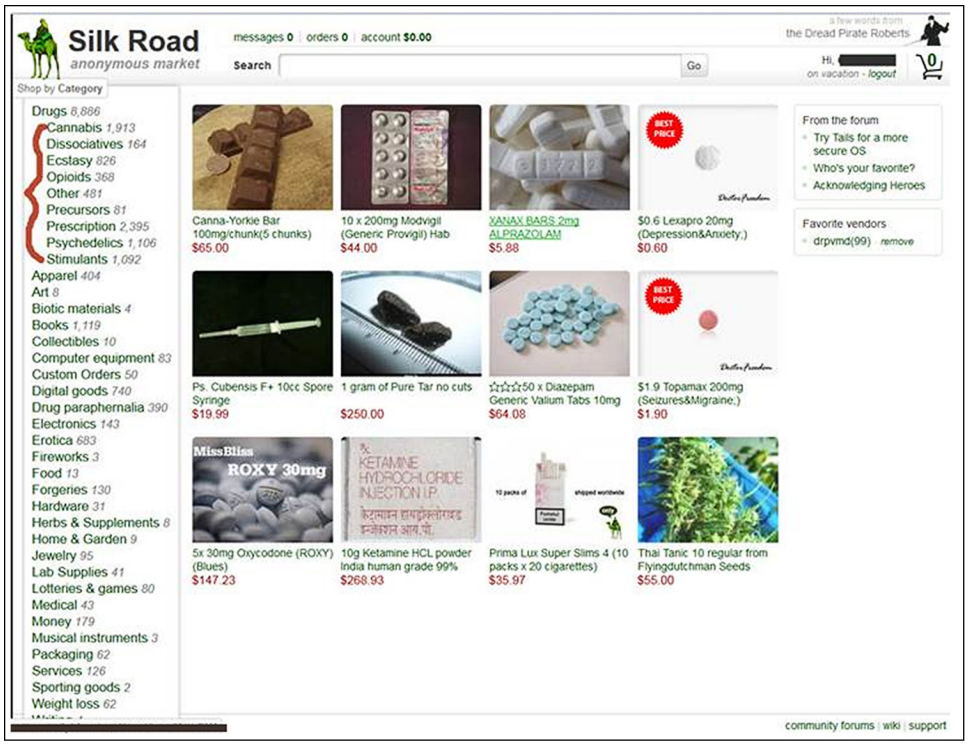
in illicit proceeds.[75] As of April 2014, this investigation had produced $40 million in seizures and had resulted in the arrests of five individuals.

- In April 2013, law enforcement agencies filed a civil asset forfeiture complaint against Tcash Ads Inc., an online payment processor that allegedly enabled users to make purchases anonymously from virtual currency exchanges, with operating an unlicensed money services business. Additionally, law enforcement agencies seized the bank accounts of Tcash Ads Inc. The Secret Service worked on the case with FinCEN and DOJ's Asset Forfeiture and Money Laundering Section.

- From October 2010 through November 2012, law enforcement agencies convicted three organizers of a worldwide conspiracy to use a network of virus-controlled computers that deployed e-mail spam designed to manipulate stock prices. The organizers paid the spammers $1.4 million for their illegal services via the centralized virtual currency e-Gold and wire transfers. Charges included conspiring to further securities fraud using spam, conspiring to transmit spam through unauthorized access to computers, and four counts of transmission of spam by unauthorized computers.

[75]This case is being prosecuted jointly by the DOJ Criminal Division's Asset Forfeiture and Money Laundering Section and the U.S. Attorney's Office for the Southern District of New York.

Figure 3: Screen Shot of the Silk Road Website



Source: U.S. Immigration and Customs Enforcement.

Law enforcement agencies have also taken other actions to help support investigations involving the illicit use of virtual currencies, including the following examples.

- The FBI has produced numerous criminal intelligence products addressing virtual currencies. These intelligence products have generally focused on cases involving the illicit use of virtual currencies, ways in which virtual currencies have been or could be used to facilitate crimes, and the related challenges for law enforcement. The FBI shares these products with foreign, state, and local law enforcement partners as appropriate.

- Through standing bilateral agreements governing the exchange of law enforcement information, ICE-HSI is arranging meetings with various international partners to exchange intelligence and garner operational support on virtual currency issues.

- ICE-HSI also developed the Illicit Digital Economy Program, which aims to target the use of virtual currencies for money-laundering purposes by defining and organizing the primary facets of the digital economy, building internal capacity, training and developing agents and analysts, engaging other agencies, and promoting public-private partnerships.

Interagency Working Groups Have Begun to Address Virtual Currencies, but Have Not Emphasized Consumer Risks or Generally Included CFPB

Federal agency efforts to collaborate on virtual currency issues have involved creating a working group specifically focused on virtual currency, leveraging existing interagency mechanisms, and sharing information through informal interagency channels. For example, in 2012, the FBI formed the Virtual Currency Emerging Threats Working Group (VCET), an interagency working group that includes other DOJ components, FinCEN, ICE-HSI, SEC, Secret Service, Treasury, and other relevant federal partners. The purpose of VCET is to leverage members' expertise to address new virtual currency trends, address potential implications for law enforcement and the U.S. intelligence community, and mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems. The VCET meets about once every 3 months.

Federal agencies have also begun to discuss virtual currency issues in existing interagency working groups that address broader topics such as money laundering, electronic crimes, and the digital economy, as follows:

- The BSA Advisory Group—which is chaired by FinCEN and includes the prudential banking regulators, Treasury, federal and state law enforcement and regulatory agencies, and industry representatives—has addressed virtual currency issues in a number of ways. In May 2013, FinCEN provided a briefing on bitcoin, and in December 2013 three stakeholders from the virtual currency industry gave presentations on their business models and regulatory challenges. In addition, the BSA Advisory Group invited a representative of the virtual currency industry to join the group in 2014.
- The Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money-Laundering Working Group—which is currently chaired by OCC and includes the prudential banking regulators and CFPB—is in the process of revising the current (2010)

FFIEC BSA/Anti-Money Laundering Examination Manual.[76] The revisions related to virtual currencies may include information on FinCEN's March 2013 guidance and regulatory expectations that depository institutions should undertake a risk assessment with a particular focus on the money laundering risks posed by new products and services.

- The Secret Service-sponsored Electronic Crimes Task Forces (ECTF) includes 35 Secret Service field offices; federal law enforcement agencies such as ICE-HSI; and members of the private sector, academia, and state and local law enforcement.[77] This group's mission is to prevent, detect, and investigate electronic crimes, including those involving virtual currency. This group has conducted computer forensics and other investigative activity on various virtual currencies and made arrests of individuals who have used virtual currencies as part of their criminal activities. This group has also held quarterly meetings on virtual currencies to discuss legal and regulatory issues and trends in crimes involving virtual currencies.

- The Digital Economy Task Force was established in 2013 by Thomson Reuters (a multinational media and information firm) and the International Centre for Missing & Exploited Children.[78] This task force includes members from both the public and private sectors. Task force members from the federal government include representatives from the FBI, ICE-HSI, Secret Service, the Department of State, and the United States Agency for International Development. This group published a report in March 2014 on the benefits and challenges of

[76]FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Federal Reserve, FDIC, NCUA, OCC, and CFPB, and to make recommendations to promote uniformity in the supervision of financial institutions.

[77]The Secret Service was mandated by the USA PATRIOT Act to establish a nationwide network of Electronic Crimes Task Forces. Pub. L. 107-56, § 105, 115 Stat 272, 277 (2001) (codified at 18 U.S.C. § 3056 note). The goal of the network is to bring together federal, state, and local law enforcement, as well as prosecutors, private industry, and academia to prevent, detect, and investigate various forms of electronic crime.

[78]The International Centre for Missing & Exploited Children is a nonprofit corporation that leads a movement to protect children from sexual exploitation and abduction. The Centre is involved in virtual currency issues because of connections between digital technologies that facilitate anonymity and commercial child pornography, sexual exploitation, and sex trafficking.

the digital economy.[79] Among other things, the report recommended continuing private and public research into the digital economy and illegal activities, investing in law enforcement training, rethinking investigative techniques, fostering cooperation between agencies, and promoting a national and global dialogue on policy related to virtual currencies.

A number of other existing interagency working groups have discussed or addressed virtual currency issues to some extent. See appendix II for more information on these groups.

Federal agencies have also started to collaborate outside of these working groups to help improve their knowledge of issues related to the emergence of virtual currencies and share pertinent information with various agencies.

- FinCEN and SEC have hosted meetings with industry representatives and consultants to discuss how virtual currency systems such as bitcoin and Ripple work and what legal, regulatory, technology, and law enforcement issues they present. These agencies have invited officials from other federal agencies to these sessions.
- FinCEN consulted with financial regulators and law enforcement agencies as it was formulating its March 2013 guidance on virtual currencies. These agencies included CFPB, CFTC, DEA, FBI, ICE-HSI, IRS, the prudential banking regulators, SEC, and the Secret Service.
- SEC notified CFTC of its review of the Winklevoss Bitcoin Trust registration statement.
- FinCEN issued a Networking Bulletin on cryptocurrencies in March 2013 to provide details to law enforcement agencies and assist them in following money moving between virtual currency channels and the traditional U.S. financial system. Among other things, the bulletin addressed the role of entities that facilitate the purchase and exchange of virtual currencies and the types of records these entities maintain that could be useful to investigative officials. Also, the Networking Bulletin elicited information from its recipients, which in turn helped FinCEN issue additional analytical products of a tactical nature to inform law enforcement operations. FinCEN has also shared

[79]Digital Economy Task Force, *The Digital Economy: Potential, Perils, and Promises* (March 2014).

this information with several regulatory and foreign financial intelligence unit partners.

- CFPB officials said they had recently conferred on virtual currency issues with a number of domestic and international regulators, including the Federal Reserve Bank of San Francisco, the Federal Trade Commission, NCUA, OCC, Treasury, New York State's Department of Financial Services, and the European Banking Authority. In addition, the officials said they had met with industry participants on these issues and conferred with interested academic and consumer group stakeholders, as well as law firms, consultancies, and industry associations.

Although there are numerous interagency collaborative efforts that have addressed virtual currency issues in some manner, interagency working groups have not focused on consumer protection issues. Rather, as previously discussed, these efforts have focused on BSA and anti-money-laundering controls and investigations of crimes in which virtual currencies have been used. In addition, CFPB's involvement in interagency working groups that address virtual currencies has been limited. GAO's key practices on collaboration state that it is important to include relevant participants in interagency collaborative efforts in order to ensure, among other things, that these participants contribute knowledge, skills, and abilities to the outcomes of the effort.[80] In addition, these key practices state that once an interagency group has been established, it is important to reach out to potential participants who may have a shared interest in order to ensure that opportunities for achieving outcomes are not missed.[81] CFPB might be a relevant participant in a broader set of collaborative efforts on virtual currencies because virtual currency systems provide a new way of making financial transactions, and CFPB's responsibilities include ensuring that consumers have timely and understandable information to make responsible decisions about financial transactions.[82] Further, CFPB's strategic goals include helping consumers

[80]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

[81]GAO, *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, GAO-14-220 (Washington, D.C.: Feb. 14, 2014).

[82]CFPB (via the Office of Financial Education) is responsible for educating and empowering consumers to make better-informed financial decisions. Pub. L. No. 111-203, § 1013(d), 124 Stat. 1376, 1970 (2010).

understand the costs, risks, and tradeoffs of financial decisions and surfacing financial trends and emergent risks relevant to consumers.

Although interagency working groups addressing virtual currencies have not focused on consumer protection issues, recent events have highlighted the risks individuals face in buying and holding these currencies. For example, notable examples of bitcoin thefts by computer hackers have occurred in the past few years, including the theft of more than 35,000 bitcoins from a virtual wallet provider in April 2013 and 24,000 bitcoins from a bitcoin exchange in September 2012.[83] More recently, in February 2014, Mt. Gox filed for bankruptcy, stating that a security breach resulted in the loss of 850,000 bitcoins, the vast majority of which belonged to its customers. These bitcoins were worth more than $460 million when Mt. Gox filed for bankruptcy.[84] Mt. Gox subsequently reported that it had found 200,000 of these bitcoins in an unused virtual wallet.

Certain parties have taken actions to inform consumers about the potential risks associated with virtual currencies, but these actions have occurred outside of federal interagency efforts and have not included CFPB. In April 2014, the Conference of State Bank Supervisors and the North American Securities Administrators Association issued joint model consumer guidance to assist state regulatory agencies in educating consumers about virtual currencies and the risks of purchasing, exchanging, and investing in virtual currencies.[85] Additionally, from February through April 2014, a number of states issued consumer alerts about virtual currencies.[86] On the international front, the European

[83]Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues* (Washington, D.C.: Dec. 20, 2013).

[84]Data from Coindesk.com. These bitcoins were worth approximately $390 million as of March 31, 2014. https://www.coindesk.com.

[85]For the Conference of State Bank Supervisors and the North American Securities Administrators Association joint model consumer guidance, see http://www.csbs.org/legislative/testimony/Documents/ModelConsumerGuidance--Virtual%20Currencies.pdf.

[86]These states include Alabama, California, Florida, Hawaii, Maryland, Massachusetts, Nevada, Washington, and Wisconsin.

Banking Authority issued a warning to consumers in December 2013 about the risks involved in buying or holding virtual currencies.[87]

Federal interagency working groups addressing virtual currency issues have not focused on consumer protection, and CFPB has generally not participated in these groups, for a number of potential reasons. For example, the extent to which individuals using virtual currencies are speculative investors or ordinary consumers is unclear, and CFPB has received few consumer complaints about these currencies.[88] In addition, incidents involving the use of virtual currencies for illicit purposes have made money laundering and other law enforcement issues primary concerns, and existing interagency working groups are primarily composed of agencies that share responsibilities for these matters. However, emerging consumer risks indicate that interagency collaborative efforts may need to place greater emphasis on consumer protection issues in order to address the full range of challenges posed by virtual currencies. Additionally, without CFPB's participation, interagency working groups are not fully leveraging the expertise of the lead consumer financial protection agency, and CFPB may not be receiving information that it could use to assess the risks that virtual currencies pose to consumers.

Conclusions

Bitcoin and other virtual currencies are technological innovations that provide users with certain benefits but also pose a number of risks. Because virtual currencies touch on the responsibilities of multiple federal agencies, addressing these risks will require effective interagency collaboration. Thus far, interagency efforts have had a law enforcement focus, reflecting the attractiveness of virtual currencies to those who may want to launder money or purchase black market items. If virtual currencies become more widely used, other types of regulatory and enforcement issues may come to the forefront. For example, recent events suggest that consumer protection is an emerging risk, as

[87]European Banking Authority, *Warning to Consumers on Virtual Currencies*, EBA/WRG/2013/01, Dec. 12, 2013. See http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies.

[88]CFPB's complaint intake system is not specifically geared towards virtual currency complaints. However, in February 2014, CFPB ran a query of its Consumer Complaint Database to determine the number of complaints that had mentioned virtual currency or bitcoin and found that only 14 out of about 290,000 complaints met that condition.

evidenced by the loss or theft of bitcoins from exchanges and virtual wallet providers and consumer warnings issued by nonfederal and non-U.S. entities. However, federal interagency working groups addressing virtual currencies have thus far not emphasized consumer-protection issues, and participation by the federal government's lead consumer financial protection agency, CFPB, has been limited. Therefore, these efforts may not be consistent with key practices that can benefit interagency collaboration, such as including all relevant participants to ensure that their knowledge, skills, and abilities contribute to the outcomes of the effort. As a result, future interagency efforts may not be in a position to address consumer risks associated with virtual currencies in the most timely and effective manner.

Recommendation for Executive Action

To help ensure that federal interagency collaboration on virtual currencies addresses emerging consumer protection issues, we recommend that the Director of CFPB (1) identify which interagency working groups could help CFPB maintain awareness of these issues or would benefit from CFPB's participation; and (2) decide, in coordination with the agencies already participating in these efforts, which ones CFPB should participate in.

Agency Comments

We provided a draft of this report to CFPB, CFTC, DOJ, DHS, FDIC, the Federal Reserve, NCUA, OCC, SEC, and Treasury for review and comment. CFPB and NCUA provided written comments, which are reprinted in appendixes III and IV. In addition, CFPB, CFTC, DHS, DOJ, the Federal Reserve, NCUA, OCC, SEC, and Treasury provided technical comments, which we incorporated into the report where appropriate.

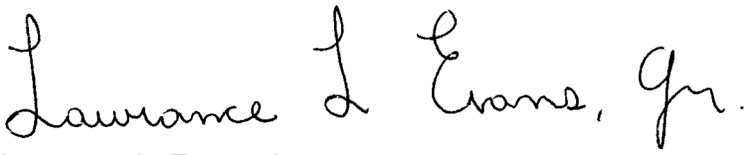
In its letter, CFPB concurred with our recommendation to identify and participate in pertinent interagency working groups addressing virtual currencies. CFPB stated that, to date, these groups have primarily focused on BSA concerns, anti-money-laundering controls, and the investigation of crimes involving virtual currencies. CFPB said that, as a result, its participation in these working groups has been limited. CFPB also stated that as consumer protection concerns have increased in recent months, its own work on virtual currencies and the work of other financial regulators in this area could benefit from a collaborative approach.

In its letter, NCUA said that the report provides a clear discussion of the risks related to virtual currencies as well as a survey of current efforts in the regulatory community to address the related policy issues. NCUA also

expressed support for increasing emphasis on consumer protection issues pertaining to virtual currencies.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to CFPB, CFTC, DOJ, DHS, FDIC, the Federal Reserve, NCUA, OCC, SEC, Treasury, interested congressional committees and members, and others. This report will also be available at no charge on our website at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-8678 or evansl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

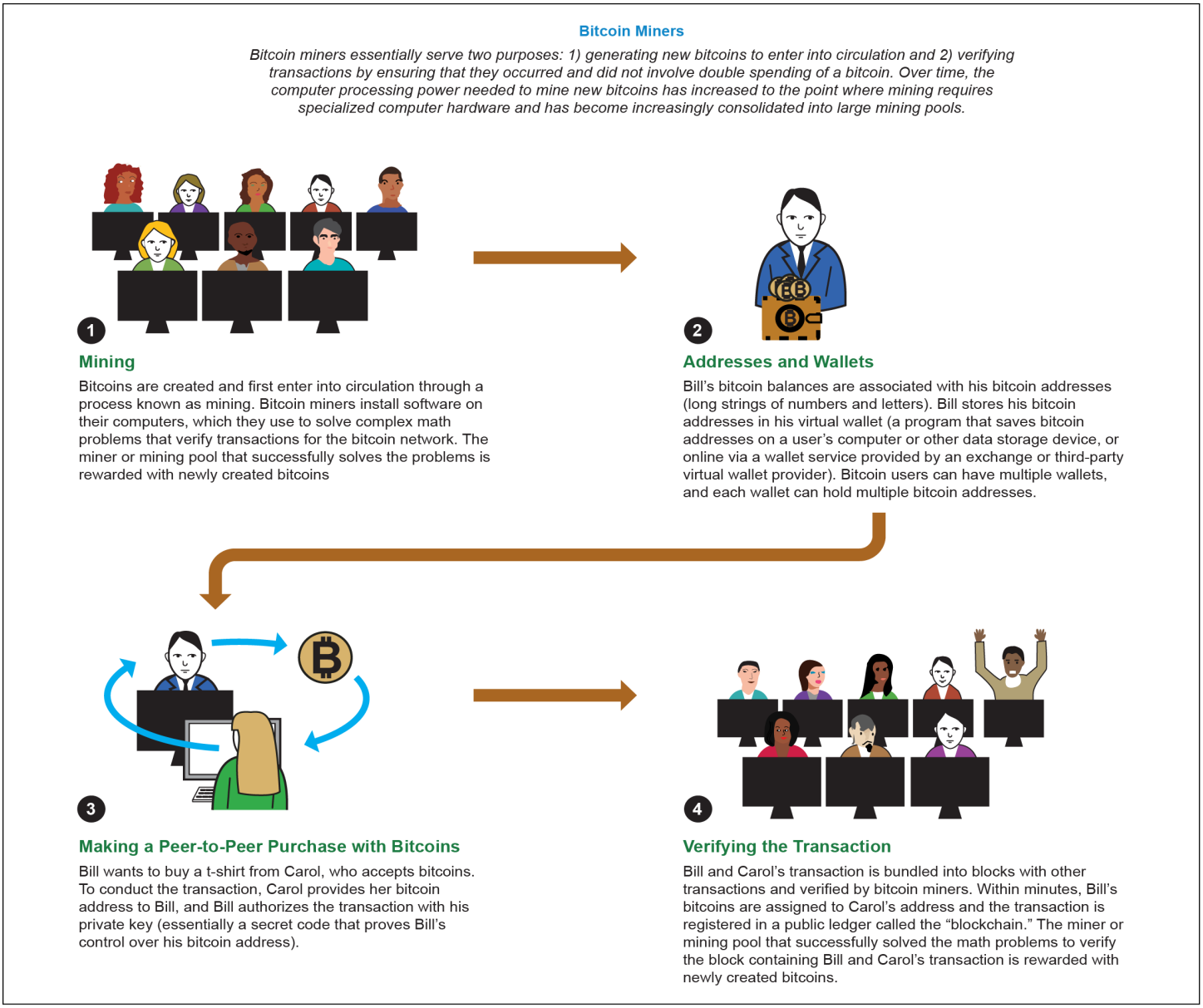


Lawrance L. Evans, Jr.
Director, Financial Markets and Community Investment

Appendix I: How Bitcoins Enter into Circulation and Are Used in Transactions

This appendix shows how bitcoins enter into circulation through "mining," how transactions are conducted, and how miners verify transactions (see fig. 4).

Figure 4: How Bitcoins Enter into Circulation and Are Used in Transactions



Source: GAO.

Appendix II: Interagency Working Groups that Have Addressed Virtual Currency Issues

In this appendix, we present some of the interagency working groups (including task forces and other interagency collaborative bodies) that have discussed virtual currency issues, and in some cases, taken specific actions. This list is based on information we obtained from the federal financial regulatory and law enforcement agencies we met with and is not intended to be an exhaustive list.

Table 1: Interagency Working Groups that Have Addressed Virtual Currency Issues, as of April 2014

Working group	Participating agencies	Mission and goals	Ways in which group addressed virtual currencies
Bank Secrecy Act Advisory Group (BSAAG)	FinCEN (lead); CFTC; DEA; DOJ Criminal Division; FBI; FDIC; Federal Reserve; ICE-HSI; IRS; NCUA; OCC; Office of National Drug Control Policy; SEC; Secret Service; and U.S. Postal Service; as well as representatives of financial institutions; trade groups; self-regulatory organizations; and state regulatory agencies.	This public-private group serves as a means by which the Secretary of the Treasury receives advice on the manner in which reporting requirements in BSA should be modified to enhance the ability of law enforcement agencies to use the information. It also informs private sector representatives of law enforcement's uses of BSA reports provided by financial institutions.	Meetings have covered issues related to virtual currencies: • The May 2013 meeting included a briefing on the bitcoin virtual currency system. • The December 2013 meeting included a panel of virtual currency industry representatives who discussed business models and regulatory compliance challenges. • In April 2014, a meeting of the BSAAG Illicit Finance Committee included a presentation on vulnerabilities and challenges related to virtual currencies, as well as opportunities to enhance collective anti-money-laundering efforts and information sharing. In addition, BSAAG invited a representative of the virtual currency industry to join the group in 2014.
Digital Economy Task Force	Thomson Reuters and the International Centre for Missing & Exploited Children (lead); FBI; ICE-HSI; Secret Service; Department of State; and United States Agency for International Development (USAID); as well as members of the private sector and academia.	This group's mission is to educate the public, work collaboratively across stakeholder groups, and balance the convenience of the digital currencies with controls to combat illegal activity.	Created in September 2013, this task force has formed working groups on such issues as safeguarding human rights; regulation; interagency coordination; and law enforcement. In March 2014, the task force published a report on the benefits and challenges of the digital economy.[a] Among other things, the report recommended private and public sector efforts to continue research into the digital economy and illegal activities; investing in law enforcement training; rethinking investigative techniques; fostering cooperation between agencies; and promoting a national and global dialogue on policy.

Working group	Participating agencies	Mission and goals	Ways in which group addressed virtual currencies
Electronic Crimes Task Forces (ECTF) and Working Groups	35 Secret Service field offices (lead) and federal law enforcement agencies such as ICE-HSI, as well as members of the private sector, academia, and state and local law enforcement.	The mission of these groups is to prevent, detect, and investigate various forms of electronic crime, including potential terrorist attacks against critical infrastructure and financial payment systems.	ECTFs address issues concerning virtual currencies as one of a variety of subjects related to the investigations into electronic crime. Specifically, ECTFs have: • conducted computer forensics and other investigative activity concerning various virtual currencies; • made arrests of individuals who have used virtual currencies as part of their criminal activities; and • discussed virtual currencies at quarterly meetings, covering topics such as types of virtual currencies and related legal and regulatory issues, trends in criminal uses, and methods for conducting investigations.
Federal Financial Institutions Examination Council (FFIEC) BSA/Anti-Money-Laundering Working Group[b]	OCC (rotating chair), CFPB; FDIC; Federal Reserve; NCUA; and the State Liaison Committee are voting members.[c]	FFIEC prescribes uniform principles, standards, and report forms for the federal examination of financial institutions by the prudential banking regulators—FDIC, Federal Reserve, NCUA, and OCC—and makes recommendations to promote uniformity in the supervision of financial institutions. Within this context, the FFIEC BSA/Anti-Money-Laundering Working Group's mission is to enhance coordination of BSA/anti-money-laundering training, guidance, and policy.	The BSA/Anti-Money-Laundering Working Group is leading the revision of the current (2010) FFIEC BSA/Anti-Money Laundering Examination Manual. Revisions related to virtual currencies may include information on FinCEN's March 2013 guidance; a brief note describing Internet-based electronic cash, which includes virtual currency; and regulatory expectations that banks should undertake a risk assessment with a particular focus on the money-laundering risks posed by new products, services, and technologies.

Working group	Participating agencies	Mission and goals	Ways in which group addressed virtual currencies
Financial Action Task Force (FATF)	FATF is an international intergovernmental organization with 36 member countries, including the U.S. Treasury as the lead agency of the U.S. delegation. Other U.S. delegation participants include DOJ's Asset Forfeiture and Money Laundering Section; DHS (including ICE-HSI); SEC; IRS; and the Department of State.	This group sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, and the financing of terrorism and proliferation.	• In February 2014, FATF developed a discussion paper on virtual currencies, which described virtual currency systems, participants, and some of the major virtual currencies such as bitcoin, and proposed a common set of terms and conceptual framework for analyzing virtual currencies. The paper also discussed the potential legitimate uses of virtual currencies, the risks these currencies may pose, and the different regulatory approaches countries are taking to address virtual currencies. The U.S. delegation prepared the paper together with delegations from Australia, Canada, Russia, and the United Kingdom. As of April 2014, the discussion paper was not yet public. • In March 2014, FATF included a discussion of virtual currencies as part of the Private Sector Consultative Forum, which included experts on virtual currencies. The group discussed how virtual currencies and their exchangers operate; the associated money laundering and terrorist financing risks; what measures countries and financial institutions are taking to assess and mitigate those risks; and what regulatory approaches are currently being taken.

Working group	Participating agencies	Mission and goals	Ways in which group addressed virtual currencies
Interagency Bank Fraud Enforcement Working Group	DOJ (Criminal Division lead, as well as the Asset Forfeiture and Money Laundering Section, Executive Office for U.S. Attorneys, Executive Office for U.S. Trustees, and FBI); CFPB; CFTC; Department of Housing and Urban Development; DHS (ICE-HSI and Secret Service); Export-Import Bank; Farm Credit Administration; FDIC; Federal Housing Finance Agency; Federal Reserve; IRS; NCUA; OCC; SEC; Treasury (Bureau of Public Debt, FinCEN, Office of Inspector General, Office of General Counsel, Office of Critical Infrastructure Protection, Office of Financial Stability, and Special Inspector General for the Troubled Asset Relief Program); U.S. Postal Inspection Service; and the District of Columbia Department of Insurance, Securities, and Banking.	This group's mission is to share information on significant trends, developments, and other issues in financial institution fraud and, as appropriate, identify and carry out projects of common interest to the working group's members.	The working group has occasionally discussed virtual currencies in the past year. Discussions to date have aimed to educate and inform members about virtual currencies. Planned activities include a presentation on the IRS notice addressing the status of virtual currencies under federal tax law. Within the Interagency Bank Fraud Working Group, the Payments Fraud Working Group has also addressed virtual currencies. The June 2013 meeting included presentations on e-Gold, the Liberty Reserve indictment, and FinCEN's guidance on how BSA regulations apply to participants in certain virtual currency systems.

Working group	Participating agencies	Mission and goals	Ways in which group addressed virtual currencies
International Organized Crime Intelligence and Operations Center (IOC-2)	DOJ (lead, including the Bureau of Alcohol, Firearms and Explosives; Criminal Division, DEA, and FBI); DHS (ICE-HSI and Secret Service); IRS-Criminal Investigation; Department of Labor (Office of Inspector General); Department of State (Bureau of Diplomatic Security); and U.S. Postal Inspection Service.	This group's mission is to significantly disrupt and dismantle transnational criminal organizations posing the greatest threat to the United States. The group does so by (1) deconflicting and analyzing transnational organized crime information and intelligence; (2) disseminating information and intelligence to support law enforcement operations, investigations, prosecutions, and forfeiture proceedings; and (3) coordinating jurisdictional and multiagency operations, investigations and prosecutions.	IOC-2 supports member-agency investigations of both virtual currency administrators that are suspected of violating U.S. law and individuals who are suspected of using virtual currencies to commit crimes. Specifically, IOC-2 assists its member agencies by: • sharing investigative details that will serve to deconflict current investigative and prosecutorial targets; • identifying current trends in the illicit use of virtual currencies; • sharing best practices in developing investigative and prosecutorial strategies; • discussing investigative challenges and solutions; • identifying tools, points of contact, and other areas of interest that offer assistance and serve as force multipliers in supporting virtual currency investigations and prosecutions; and • creating cross-agency relationships for future cooperation and coordination on virtual currency issues, investigations, and prosecutions.

Working group	Participating agencies	Mission and goals	Ways in which group addressed virtual currencies
Terrorist Finance Working Group's New Payments Systems Ad Hoc Working Group	Department of State (lead, including the Bureaus of Economic and Business Affairs, Counterterrorism, and International Narcotics and Law Enforcement Affairs); Department of Defense; DOJ (Asset Forfeiture and Money Laundering Section; Criminal Division; DEA; FBI; National Security Division; and Office of Overseas Prosecutorial Development, Assistance and Training); FDIC; Federal Trade Commission; ICE-HSI; IRS-Criminal Investigation; Treasury (FinCEN, Office of Terrorism and Financial Intelligence, and Office of Technical Assistance), and USAID.	The larger working group's mission is to coordinate counter-terrorism-financing and anti-money-laundering training and technical assistance programs to countries deemed most vulnerable to terrorist financing. Within this context, the New Payments Ad Hoc Working Group's mission is two-fold: (1) to help ensure that foreign partners providing assistance and capacity building have a baseline understanding of new payment systems and the counter-terrorism-financing and anti-money-laundering risks and vulnerabilities that they may pose, and (2) to collaborate with other federal agencies and appropriate public and private sector entities to develop training and technical assistance programs in line with international standards set by groups such as FATF.	The New Payments Ad Hoc Working Group, which formed in 2013 and meets every two to three months, has addressed the use of virtual currencies at several meetings. Topics have included: • briefings on virtual currencies, how they operate, and risks; • the set of common virtual currency vocabulary terms proposed in the FATF's discussion paper on virtual currencies; • trainings that ad hoc working group participants plan to offer through 2015 on counter-terrorism-financing and anti-money-laundering risks associated with virtual currencies. • workshops that the Department of State, USAID, and other ad hoc working group participants offered in 2013 and 2014 on new payment systems—including virtual currencies—to foreign partners in the East Africa, Southeast Asia, Latin America, and the Caribbean. • the ways in which other interagency collaborative groups—such as the Egmont Group, which is composed of FinCEN and financial intelligence units from other countries—are addressing virtual currencies.
Virtual Currencies Emerging Threats Working Group	DOJ (FBI lead and other DOJ components); FinCEN; ICE-HSI; SEC; Treasury; Secret Service; and other relevant federal partners.	To address the illicit use of virtual currencies.	This group leverages members' expertise to address new virtual currency trends, address potential implications for law enforcement and the U.S. intelligence community, and mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems.

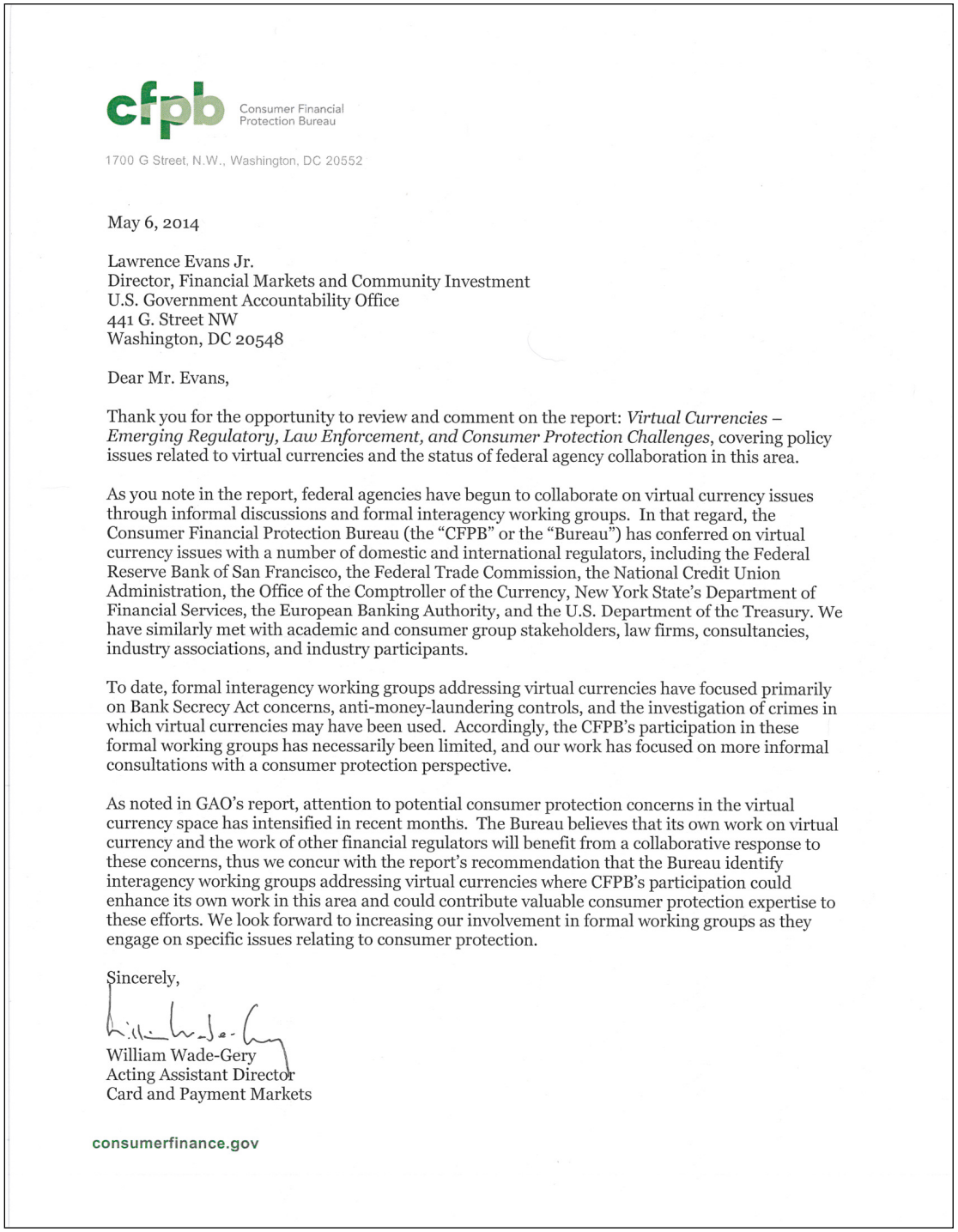
Source: GAO analysis of agency interviews and documents, as well as websites of interagency collaborative efforts.

[a]Digital Economy Task Force, *The Digital Economy: Potential, Perils, and Promises* (Mar. 2014).

[b]FDIC, the Federal Reserve, and NCUA told us that the FFIEC Taskforce on Supervision, and the Taskforce's Information Technology Subgroup, have also discussed virtual currencies.

[c]The FFIEC State Liaison Committee includes representatives from the Conference of State Bank Supervisors, the American Council of State Savings Supervisors, and the National Association of State Credit Union Supervisors. Other FFIEC BSA/Anti-Money-Laundering Working Group non-voting members include CFTC; FinCEN; IRS; SEC; Treasury's Office of Foreign Assets Control; and Treasury's Office of Terrorist Financing and Financial Crimes.

Appendix III: Comments from the Consumer Financial Protection Bureau



cfpb Consumer Financial Protection Bureau

1700 G Street, N.W., Washington, DC 20552

May 6, 2014

Lawrence Evans Jr.
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G. Street NW
Washington, DC 20548

Dear Mr. Evans,

Thank you for the opportunity to review and comment on the report: *Virtual Currencies – Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, covering policy issues related to virtual currencies and the status of federal agency collaboration in this area.

As you note in the report, federal agencies have begun to collaborate on virtual currency issues through informal discussions and formal interagency working groups. In that regard, the Consumer Financial Protection Bureau (the "CFPB" or the "Bureau") has conferred on virtual currency issues with a number of domestic and international regulators, including the Federal Reserve Bank of San Francisco, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, New York State's Department of Financial Services, the European Banking Authority, and the U.S. Department of the Treasury. We have similarly met with academic and consumer group stakeholders, law firms, consultancies, industry associations, and industry participants.

To date, formal interagency working groups addressing virtual currencies have focused primarily on Bank Secrecy Act concerns, anti-money-laundering controls, and the investigation of crimes in which virtual currencies may have been used. Accordingly, the CFPB's participation in these formal working groups has necessarily been limited, and our work has focused on more informal consultations with a consumer protection perspective.

As noted in GAO's report, attention to potential consumer protection concerns in the virtual currency space has intensified in recent months. The Bureau believes that its own work on virtual currency and the work of other financial regulators will benefit from a collaborative response to these concerns, thus we concur with the report's recommendation that the Bureau identify interagency working groups addressing virtual currencies where CFPB's participation could enhance its own work in this area and could contribute valuable consumer protection expertise to these efforts. We look forward to increasing our involvement in formal working groups as they engage on specific issues relating to consumer protection.

Sincerely,

William Wade-Gery
Acting Assistant Director
Card and Payment Markets

consumerfinance.gov

Appendix IV: Comments from the National Credit Union Administration

National Credit Union Administration

Executive Director

May 1, 2014

Lawrance L. Evans, Jr.
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Evans:

We reviewed the U.S. General Accountability Office's report entitled *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges (GAO-14-496)*.

The report provides clear discussion of the risks related to virtual currencies as well as a survey of current efforts in the regulatory community to address the related policy issues. We support the report's recommendation to increase emphasis on consumer protection issues going forward. In NCUA's limited dealings with virtual currencies, we have consistently focused on consumer protection as well as safety and soundness.

Thank you for the opportunity to comment.

Sincerely,

Mark Treichel
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 - 703-518-6320

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Lawrance L. Evans, Jr. (202) 512-8678 or evansl@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Steve Westley (Assistant Director), Bethany Benitez, Chloe Brown, Anna Chung, Tonita Gillich, José R. Peña, and Robert Pollard made key contributions to this report. Also contributing to this report were Jennifer Schwartz, Jena Sinkfield, Ardith Spence, Andrew Stavisky, and Sarah Veale.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548